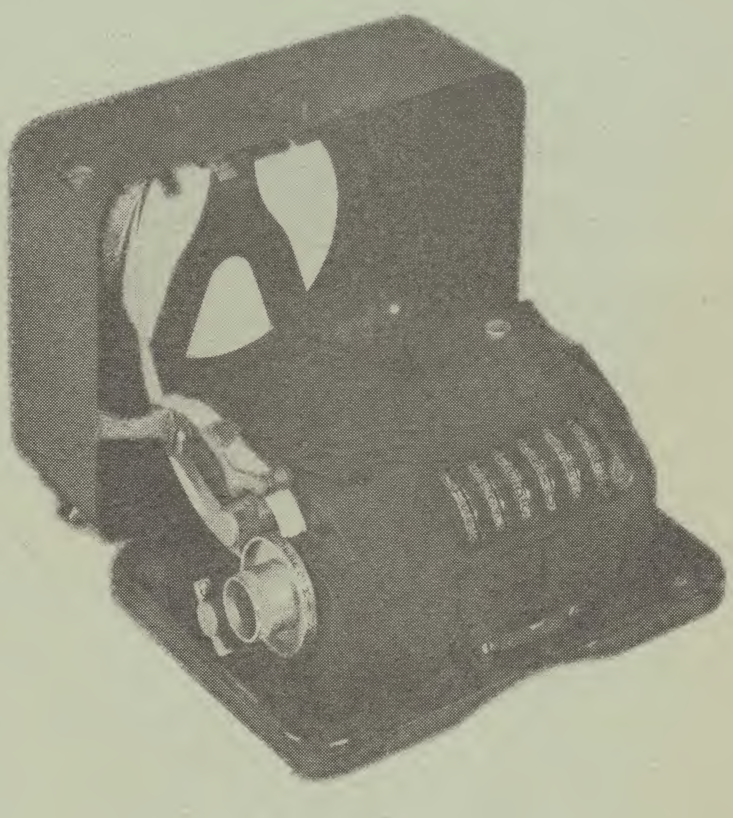
A CRYPTOGRAPHIC SERIES

17

CRYPTANALYSIS Of The HAGELIN CRYPTOGRAPH



by

Wayne G. Barker

From Aegean Park Press

CRYPTANALYSIS Of The HAGELIN CRYPTOGRAPH

by

Wayne G. Barker

ISBN: 0-89412-022-0

Published by AEGEAN PARK PRESS
P.O. Box 2837, Laguna Hills, California 92653

Manufactured in the United States of America

CRYPTANALYSIS Of The HAGELIN CRYPTOGRAPH

PREFACE

The author has spent several years writing this book. Many hours have been spent, writing, re-writing, and correcting, always attempting to insure that the material presented is readable, easy to understand, and especially, that the contents are cryptanalytically correct. Many hours, too, were spent preparing and checking the numerous problems that accompany most of the chapters. The problems not only will hopefully provide the reader with "many hours of enjoyment", but also will serve to reinforce in the reader's mind the knowledge learned; for after all, there is no better way to learn than by doing! Thus, the reader should conscientiously attempt to solve at least several of the problems at the end of each chapter. By the time the last chapter is finished, the reader then should indeed have a good knowledge of the cryptanalysis of the HAGELIN CRYPTOGRAPH system.

As the reader will quickly find, even after the first chapter, the HAGELIN CRYPTOGRAPH system is a fascinating problem for the cryptanalyst. There are a number of different facets in the cryptanalytic solution of the HAGELIN CRYPTOGRAPH, some simple, and some deeply complicated. Unfortunately for the amateur cryptanalyst, the practical analysis of HAGELIN CRYPTOGRAPHIC "traffic" probably requires the use of a modern computer. Nonetheless, however, there is still much that can be done simply with a piece of paper and a pencil to solve the system.

The author has been assisted by a number of persons in the preparation of this book. Some provided constructive comments, others checked pages, and some prepared enciphered messages for the author to analyze, solve, etc. Especially, the author would like to give thanks to Cipher Deavours, Brian Winkel, Herb Baruch, Louis Kruh, and Greg Mellen, each, incidentally, an outstanding cryptanalyst in his own right, for their kind help. Thanks, too, should go to David G. Cantor of the University of California, Los Angeles, and William F. Donoghue, Jr. of the University of California, Irvine, for their help with respect to a mathematical problem concerning the indicators of the HAGELIN CRYPTOGRAPH. A special thanks, also, must go to Roger Stuart Brown, not only a fine medical doctor, but also an astute *cryptologist*, for his particular assistance with respect to the HAGELIN CRYPTOGRAPH, Model Type CD-57, the subject of Chapter 10.

Finally, any errors that might have inadvertently occurred, hopefully there will not be many, are those of the author; and readers, of course, are encouraged to provide comments to the author regarding the material presented. It is the author's sincere hope that this book will contribute something to the science of *cryptology*, and that readers will find hours of enjoyment as they study the cryptanalysis of the HAGELIN CRYPTOGRAPH.

Mission Viejo,
California, 1977

WGB

INTRODUCTION

The HAGELIN CRYPTOGRAPH was invented in the 1930's, just before World War II, by a creative genius, Boris Hagelin, then of Stockholm, Sweden. Of the many "cryptographic machines" that have appeared on the cryptographic scene in the last 40 to 50 years, none have been "accepted" like the HAGELIN CRYPTOGRAPH. Indeed, the HAGELIN CRYPTOGRAPH stands alone, well above all others, when it comes to "favorable reception" by governments for their own secret communications! Even today, it is probable that the HAGELIN finds active use in many countries for both military and diplomatic communications. It would be hard to estimate in numbers "how many" Hagelin machines have actually been produced since Boris Hagelin made his first prototype machine. Perhaps as many as 500,000 machines! In any case, it can be said that many thousands of these *cryptographs* have been manufactured; and at the present time the HAGELIN CRYPTOGRAPH is manufactured and marketed by a very reputable Swiss firm: *Crypto Aktiengesellschaft, 10 Weinbergstrasse, Zug, Switzerland*.

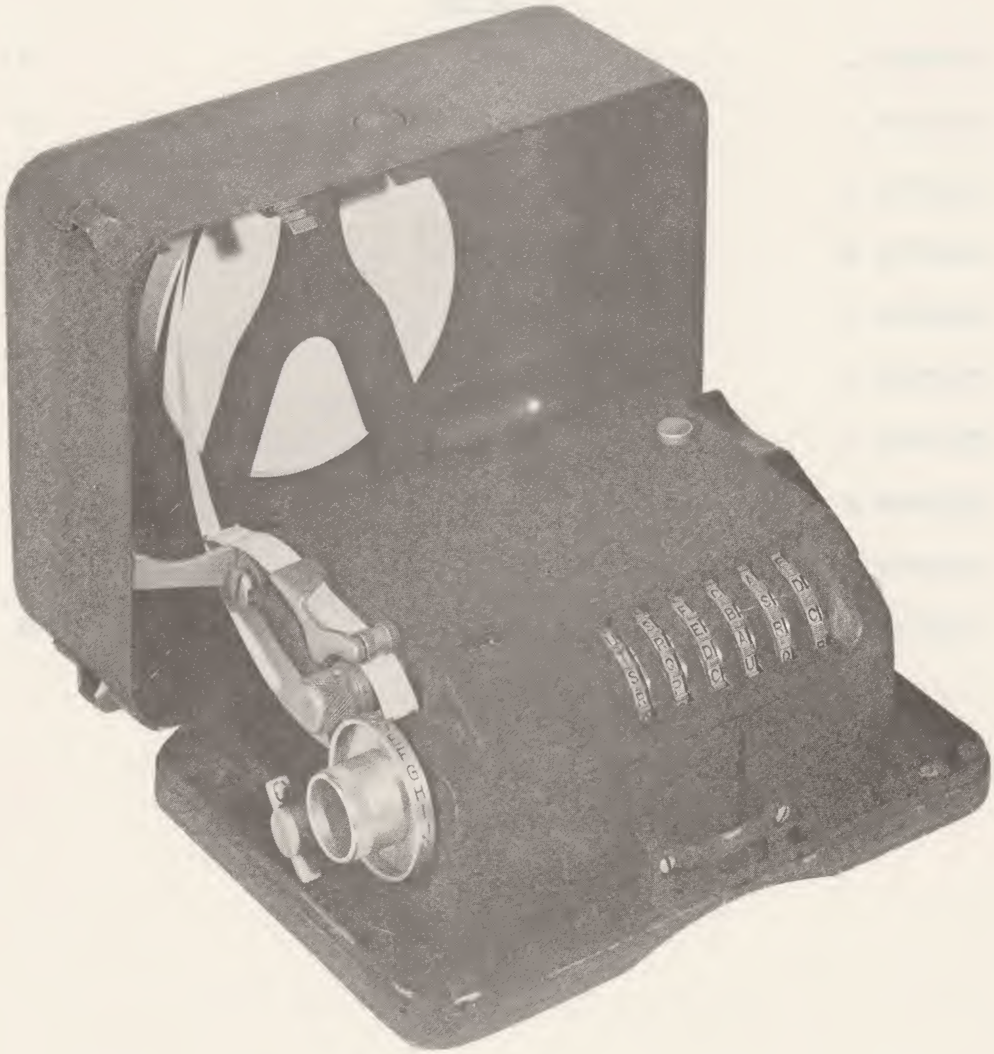
In its original form the HAGELIN CRYPTOGRAPH was a light-weight, compact, hand-operated mechanical device used for the encipherment and decipherment of messages. Shortly thereafter the output of the cryptographic machine was made to print on a gummed tape with the ciphertext conveniently divided into five-letter groups and the plaintext in normal word-lengths, the latter accomplished by using the letter "z" as a spacer between words.

Since development of the first HAGELIN CRYPTOGRAPH, then designated as the Model Type C-36 machine, with five keywheels and fixed *lugs*, a number of newer and so-called improved models have been produced.

Historically — in the United States the HAGELIN CRYPTOGRAPH is probably best known as the U.S. Army's *Converter M-209* or the U.S. Navy's *CSP-1500*. Both similar, these drab-green versions of the HAGELIN designated Model Type C-48 cipher machine, used during World War II, contained 54 movable *lugs*, two *lugs* on each of 27 *lug-bars*, and six keywheels having respectively 26, 25, 23, 21, 19, and 17 *pins*.

More recent and improved versions of the HAGELIN CRYPTOGRAPH are electrical, rather than mechanical, and contain keyboards to make encipherment and decipherment operations easier for "cryptographic clerks". Thus, for example, the older Model Type C-48 cipher machine has been replaced by the HAGELIN

LIST OF PROBLEMS



The U.S. Army's Converter M-209

Chapter 1

THE CRYPTOGRAPHIC PROCESS

When the HAGELIN CRYPTOGRAPH is actually used, encipherment and decipherment processes are performed, of course, mechanically "by the machine". For the purpose of cryptanalysis, however, we must consider the equivalent "on paper" processes of the cryptographic machine.

Essentially, during encipherment a generated key is applied to plaintext in order to obtain resultant ciphertext; and during decipherment the same generated key is applied to the ciphertext in order to obtain the original plaintext.

In the cryptographic processes of the HAGELIN CRYPTOGRAPH there are, thus, three elements to be considered:

(1) Plaintext.

(2) Ciphertext.

(3) Key.

Given any two elements, the third element may be found!

Thus --

(1) During encipherment, plaintext enciphered with key results in ciphertext.

(2) During decipherment, given the ciphertext and key, plaintext is found.

(3) And important from the viewpoint of the cryptanalyst, given ciphertext with the plaintext known, the key may be recovered.

Let us examine now the method by which the three elements, plaintext, ciphertext, and key, cohere.

The important tableau of Figure 1, known historically to the cryptographer as a *Beaufort Tableau*, provides the "relationship" between ciphertext, plaintext, and key in the HAGELIN CRYPTOGRAPH system.

The student should note that the key is a *numerical key* composed of the numbers Ø thru 27; and he should note, too, that the numbers 1 and 27 are equivalent, as are the numbers Ø and 26.

HAGELIN TABLEAU

Beaufort Tableau for the Type C-48 Cipher Device (M-209)

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	0/26	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
	1/27	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
	2	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
	3	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D
	4	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E
	5	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F
	6	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G
	7	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H
	8	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I
	9	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
	10	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K
	11	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
	12	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M
	13	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
KEY	14	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O
	15	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P
	16	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q
	17	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R
	18	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S
	19	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T
	20	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U
	21	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V
	22	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W
	23	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X
	24	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y
	25	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z

Figure 1

In the problems following this chapter the student will gain proficiency in the use of the Hagelin Tableau of Figure 1.

One special note is important, however, which concerns plaintext enciphered with the HAGELIN CRYPTOGRAPH. In order to obtain "spacing" between words - making the plaintext more easily readable - the HAGELIN CRYPTOGRAPH is designed so that the plaintext letter Z prints as a space. Thus, for example, in the HAGELIN CRYPTOGRAPH system, to the cryptanalyst plaintext might appear as follows:

HELPZNEEDEDZONZHILLZSIXZONEZZEROZZERO

But the same text, using the HAGELIN CRYPTOGRAPH, will print on gummed tape as:

HELP NEEDED ON HILL SIX ONE ERO ERO

Note that when the letter Z actually does occur in the message text, it appears as a space and must be read into the text.

Therefore, in the following problems, keep in mind that the letter Z acts as a space between words.

PROBLEMS

1. Given the keying sequence "5 26 12 19 Ø 27 6 5 Ø 21 8 4 Ø 5 13", decipher the following message:

   N V S Y I   N G L L V   G D H A N.

2. Given the key "Ø 6 6 Ø Ø Ø 6 Ø 6 Ø Ø 6 6 Ø 6 Ø 6 6 Ø 6", decipher the following message:

   U L O M R   H Y A X M   U R O N F   G X R M G.

3. Given the plaintext "SEND MORE SUPPLIES", recover the key used to encipher the following message:

   H D M W I   N T I D I   H N K S O   Z D P A I.

4. It is believed that the following ciphertext message begins with the word "REPEAT". Can you read the message?

   I V K V Z   G A O Z H   G A N V H   H Z T V A.

5. The following two messages have been enciphered with the same key. The first message begins with the word "PLEASE". Read both messages.

No. 1 - K U B Z N B A H B M C A S V U K G A G A.

No. 2 - Z T T F S X G R R M G R H A N S R I M A.

6. The following three messages have been enciphered with the same key. Message No. 2 is known to begin with the word "CONTACT". Read the messages.

No. 1 - P B J S I T H A F E S R P B W G M J A W
Z E Z R O.

No. 2 - X R A O H L G A U T V G I J R M G I V A
V V J G O.

No. 3 - L S J I H F I X O H I G I U L N U I G Z
W H J G O.

7. The following message has been enciphered with a keying sequence which repeats every 17 letters. The message is known to begin with the word "ENEMY". Read the message.

V W F N B K U V S H V R A J I V K I F Q I V J G B
W D A N V K Z I F A B W A T V L G K R S J K F A A.

8. This message, like the previous message, has been enciphered with a keying sequence which repeats every 17 letters. The message begins with the word "RESCUE". Read the message.

I C H X M V H S B A B R L V H U V M H L M H S Y V
V A O R J A N K L A H V I S A Z G O A F V C M H C
U U C X G C W H O N L R A F F N H L M C A N G M H
Y O A Y M H H C P R L M H A E L T D Y G Y L T A H.

9. The following three messages have been enciphered with the same key. The first message begins with the plaintext word "NEED". Read the messages.

No. 1 - M X V B D S X R K F L I U X U Q E A F C.

No. 2 - H X M B D N N L V F B Q Q F R T J R Q O.

No. 3 - I X K Q L G C U H F O Y W Z L T H V F C.

10. The following messages have been enciphered with the same keying sequence. Message No. 3 begins with the word "TO". Read the messages. (How might the letter Z, used as a null to complete the last group of a message, help towards solution?)

No. 1 - MTHDE GWBTF VPLDG EZVTK GUAIF
CPAIZ WGJYW GRXEI KGHIA.

No. 2 - BTMQA CVNOH TKAQX LTVBV GRWAU
SOAVV OWILQ BJQOI BNCII KKKZT.

No. 3 - GTHBV BVOGW AWNAM BNDXX UAWVU
DIBYF PZWAH SAMRY OGNTW OBPAN.

No. 4 - DDHPG GOUHL RDOJO EWFXR BACLQ
CIGEN KAPYC QRBKM KBHIA.

No. 5 - HNRSO QARBI ZCNOS ATRRV GRWAM
CQBNO ADJXQ BINVN BCLZH KAPAN.

No. 6 - GLSIN KMGWZ ODVFG QECGM RFBWD
DIUEE KAWEJ WASTN.

Chapter 2

ANALYSIS OF A SINGLE-WHEEL HAGELIN CRYPTOGRAPH

The *cryptographic security* basically inherent in the HAGELIN CRYPTOGRAPH system is provided principally by the manner in which key is generated.

Though the actual HAGELIN CRYPTOGRAPH consists of a number of wheels, most often six, each of which contributes normally its part to the final generated key, for the purpose of introducing the student to the principle behind "key generation" in the HAGELIN CRYPTOGRAPH, we shall consider in this chapter a keying sequence being generated by a single wheel.

The student should understand, however, that though a single-wheel HAGELIN CRYPTOGRAPH system is somewhat "mythical", in that it is very unlikely that such a system would actually be encountered, such a system is within the realm of possibility and can in fact be duplicated with any HAGELIN CRYPTOGRAPH by merely putting the remaining wheels in a non-effective condition.

Each wheel of the HAGELIN CRYPTOGRAPH is of given length; or to put it another way, each wheel has a given number of *pin* positions. As letters are enciphered (or deciphered), the wheels simultaneously revolve step-by-step, one position to the next. Thus, a wheel, for example, having 17 positions, or *pins*, after encipherment of 17 letters will have returned to its original position.

Two mechanical variables affect key generation in the HAGELIN CRYPTOGRAPH system, *lug-settings* and *pin-settings*; and these variables are set on wheels before encipherment (or decipherment) by the cryptographic clerk.

First, a number of *lugs* may be made effective for each wheel. The number of *lugs* set on a wheel may be one, two, three, or even twelve, thirteen, etc. If no *lugs* are set on a wheel, the wheel will be in a non-effective condition.

Second, each position of a wheel may be made effective or non-effective by pushing a *pin* to the right or to the left. If a *pin* is pushed to the left, the position becomes non-effective; if a *pin* is pushed to the right, the position becomes effective.

When a position on the wheel is effective, when its "pin" is to the right, the key generated by the wheel will be equal to the number of "lugs" set on the wheel. When a position on the wheel is non-effective, the key will be Ø. Thus, for example, the key generated from a wheel of 17 positions might look as follows:

Ø 8 8 8 Ø Ø 8 Ø 8 Ø 8 Ø Ø 8 8 Ø 8 Ø 8 8 8 Ø Ø 8 Ø 8 . . . etc.

It can be seen that in this generated keying sequence the number of "lugs" set on the wheel is eight; that in the first position, the "pin" is in a non-effective position; that in the next three positions, the "pins" are effective, etc. After 17 numbers of key, the keying sequence, of course, repeats.

Cryptanalysis of a single-wheel HAGELIN CRYPTOGRAPH system is rather easy, for the generated keying sequence always consists of a combination of but two numbers, one of the numbers being Ø, representing a "pin" in a non-effective position.

Consider, for example, the cryptanalysis of the following message known to be enciphered with a single-wheel:

Y V X L M   G A L U V   C G X A N   P F V Q R   W A C V N
L H H P I   B A W B A   X G B K A   W Y Z C H   D R W G H
C T A P G   A M H J S   W A Q A A.

As the message has been enciphered with a single-wheel, we know that the generated keying sequence consists of the number Ø plus one other number. We might use a "trial-and-error" method, and simply assume what the other number might be; but there might be an easier method to determine the other number.

Since the letter Z is used in the HAGELIN CRYPTOGRAPH method as a "spacer" between words, we might consider also the final group of the message. In order to complete the last five-letter group of the message, is it possible that the letter Z was used as a <u>null</u>?

Let us therefore examine the last group of the message, and make the assumption that the message ends with one or more Z's:

ciphertext:	W	A	Q	A	A
assumed plaintext:	Z	Z	Z	Z	Z
resulting key:	22	Ø	16	Ø	Ø

We may disregard the ciphertext letter W, for it probably represents the last letter of the message; but the last four letters appear likely to represent Z's. Further, it appears that the generated key probably consists of the numbers Ø and 16.

Let us, therefore, attempt to read the message, assuming that the "lug setting" for the wheel is 16.

For the first 20 letters of ciphertext, let us examine the plaintext possibilities:

```
                  Ciphertext:  Y V X L M G A L U V C G X A N P F V Q R
   If key is Ø, plaintext is:  B E C O N T Z O F E X T C Z M K U E J I
  If key is 16, plaintext is:  R U S E D W P E V U N K S P C A K U Z Y
```

Within these possibilities, can plaintext be read? The letter Z, used as a "spacer" between words, proves especially valuable to separate potential words:

```
B E C O N T Z O F E X T C Z M K U E J I
R U S E D W P E V U N K S P C A K U Z Y
```

yields

```
B E C O N T   O F E X T C   M K U E   I
R U S E D W   E V U N K S   C A K U   Y
```

And the plaintext is evident:

```
B E C O N T   O F E X T C   M K U E   I
R U S E D W   E V U N K S   C A K U   Y
```

or

```
R E C E N T   E V E N T S   M A K E   I(T) . . .
```

In the problems that follow, messages can be analyzed in similar fashion. Where the last group does not reveal the unknown "other" number of the generated key, the solver can fall back on the "trial-and-error" method of testing the limited number of "other" numbers possible.

PROBLEMS

11. The following two messages contain the same plaintext, but have been enciphered with different "wheel settings". Read the messages.

No. 1 - T B H N Z   Z V A N X   I G M R G   M B D H G   H B M A G.

No. 2 - U V O H G   T V H H R   J H T L H   M C K H A   I V N H H.

12. The following messages have been enciphered using the same keying sequence. Read the messages.

No. 1 - W V L J R   S V W A U   D Z A L Z   H J H A Z   I A G F I
J V A U L   W Z P A O.

No. 2 - Y O J N H   J A Z W S   R V V O R   U O Z I U   F O O J I
P O H T K   K L W G O   D F O O O   Y V O I F   I A R V G
V K A A A.

13. Solve the following cryptogram:

I H T F A   G T A L R   I M K E L   G X T U Z   W S N M L
Q V U A E   R O A A S   D V A E H   A E F Y I   I H W M R
Y W R J Z   S V A H M   H N N A E   L H M K R   O A V W M
Y L X P M.

14. Read the following message:

Q V K K Z   T Y A X L   F L G Y Y   M A L V N   Y C G D O
C H J D N   V K H C T   V D A D D.

15. Solve the following:

T V V L T   G A K O Z   A C M F L   I N K R R   W X A L A.

16. Read the following cryptogram:

L L F X Q   T L R V O   F H S R L   S F N V L   F N R A L
L A D Z M   V F A F F.

17. Read the following message:

O L C J R   V M A N U   C I Z M P   J C S X K   V C A A C.

18. Solve the following:

K P A B L   R N D M W   V M X E L   Y Y R B Z   I E U V I
L G A C Z   K K Z S V   L Q E Z Q   H H V M A   R L A Q Z
T D K R I   Z A E A E.

19. Read the following message:

G T W I W   B S A I B   Y W V N A   M M A W F   R X W M Y
W B L V A   O R M W H   B S M B M   F J B I V   Y G M I A.

20. The following messages contain the same text, but keys are different. Read the messages.

No. 1 - U L A F Z   P F Z W G   Z V P I G   T W H B A.

No. 2 - P O A A Z   K I C O J   R V K A J   O W Z E D.

Chapter 3

ANALYSIS OF A TWO-WHEEL HAGELIN CRYPTOGRAPH

Let us consider in this chapter the analysis of a two-wheel HAGELIN CRYPTOGRAPH system. While it is true that a two-wheel HAGELIN CRYPTOGRAPH system, like that of a single-wheel HAGELIN CRYPTOGRAPH system, is not likely to be actually encountered, such a system is not an absolute impossibility, for it can be duplicated using the HAGELIN CRYPTOGRAPH with the remaining wheels in a non-effective condition. The remaining wheels may be put in a non-effective condition by either:

(1) putting all *pins* of the remaining wheels to the left, their non-effective position, or

(2) by failing to put *lugs* on the remaining wheels.

To introduce the student to the principle of a keying sequence being generated from more than one wheel, consider a single wheel of length 17 which produces, for example, the key "2 Ø 2 Ø 2 2 Ø 2 Ø 2 Ø 2 2 Ø 2 2 Ø". At the same time, consider a second wheel, this one of length 19, which produces, for example, the key "Ø 3 Ø 3 3 Ø Ø 3 Ø 3 3 3 Ø Ø 3 Ø 3 Ø 3".

In a two-wheel HAGELIN CRYPTOGRAPH system, these two wheels, each of different length, can combine to generate a resultant keying sequence as follows:

```
        Key #1:  2 Ø 2 Ø 2 2 Ø 2 Ø 2 Ø 2 2 Ø 2 2 Ø/2 Ø 2 Ø 2 2 Ø 2 Ø 2 Ø
        Key #2:  Ø 3 Ø 3 3 Ø Ø 3 Ø 3 3 3 Ø Ø 3 Ø 3 Ø 3/Ø 3 Ø 3 3 Ø Ø 3 Ø
                 ---------------------------------------------------------
 Resultant key:  2 3 2 3 5 2 Ø 5 Ø 5 3 5 2 Ø 5 2 3 2 3 2 3 2 5 3 2 Ø 5 Ø

                 2 2 Ø 2 2 Ø/2 Ø 2 Ø 2 2 Ø 2 Ø 2 Ø 2 2 Ø 2 2 Ø/2 Ø . . .
                 3 3 3 Ø Ø 3 Ø 3 Ø 3/Ø 3 Ø 3 3 Ø Ø 3 Ø 3 3 3 Ø Ø 3 . . .
                 -----------------------------------------------------
                 5 5 3 2 2 3 2 3 2 3 2 5 Ø 5 3 2 Ø 5 2 3 5 5 Ø 2 3 etc.
```

Note that the resultant key consists of four different numbers, Ø, 2, 3, and 5, the latter 5 resulting from the sum of 2 and 3.

We can say, then, that where a two-wheel HAGELIN system is used in this fashion, the resultant, generated key will consist of four numbers, Ø, x, y, and z, where $x + y = z$.

It should be noted, too, that the resultant keying sequence will itself not repeat until the "lowest common multiple" of the lengths of the

two wheels is reached, in this case 323 letters, the "lowest common multiple" of 17 and 19.

Let us turn to the analysis of a cryptogram produced from a keying sequence generated from two wheels in the above fashion. To make our analysis simpler, let us say, too, that the message is known to begin with the word "TO".

```
QPGDV  WVIJO  KHTBK  SGLXM  ANVFW
WZCAE  LPOAT  BOUFW  KMHVA  RXLNR
WZEAG.
```

Knowing that the first word of the message is "TO" enables us to easily recover the first three numbers of the keying sequence:

```
     Plaintext:  T  O  Z
    Ciphertext:  Q  P  G
Recovered key:  10  4  6
```

The recovered key, 10 4 6, at this point looks good; for the three numbers have the favorable property that 4 + 6 = 10. Indeed, with the known Ø in the keying sequence, we probably know all four of the numbers which comprise the resultant, generated key: Ø, 4, 6, and 10.

With the <u>four</u> numbers of the keying sequence probably identified, the four possible plaintext equivalents for each ciphertext letter may be placed beneath the letters of the cryptogram:

```
    Q P G D V W V I J O K H T B K S G L X M A N V F W W Z C A E L P O A
 Ø: J K T W E D E R Q L P S G Y P H T O C N Z M E U D D A X Z V O K L Z
 4: N O X A I H I V U P T W K C T L X S G R D Q I Y H H E B D Z S O P D
 6: P Q Z C K J K X W R V Y M E V N Z U I T F S K A J J G D F B U Q R F
10: T U D G O N O B A V Z C Q I Z R D Y M X J W O E N N K H J F Y U V J

    T B O U F W K M H V A R X L N R W Z E A G.
 Ø: G Y L F U D P N S E Z I C O M I D A V Z T
 4: K C P J Y H T R W I D M G S Q M H E Z D X
 6: M E R L A J V T Y K F O I U S O J G B F Z
10: Q I V P E N Z X C O J S M Y W S N K F J D
```

At this point, assuming the <u>four</u> key numbers to be correct, a successful solution is fairly well assured.

Again, the plaintext letter Z, the "spacer" between words, is valuable to identify word lengths, though some Z's may occur by accident. Thus,

locations of Z's are identified in columns:

	Q	P	G	D	V	W	V	I	J	O	K	H	T	B	K	S	G	L	X	M	A	N	V	F	W	W	Z	C	A	E	L	P	O	A
Ø:	J	K	T	W	E	D	E	R	Q	L	P	S	G	Y	P	H	T	O	C	N	Z	M	E	U	D	D	A	X	Z	V	O	K	L	Z
4:	N	O	X	A	I	H	I	V	U	P	T	W	K	C	T	L	X	S	G	R	D	Q	I	Y	H	H	E	B	D	Z	S	O	P	D
6:	P	Q	Z	C	K	J	K	X	W	R	V	Y	M	E	V	N	Z	U	I	T	F	S	K	A	J	J	G	D	F	B	U	Q	R	F
10:	T	U	D	G	O	N	O	B	A	V	Z	C	Q	I	Z	R	D	Y	M	X	J	W	O	E	N	N	K	H	J	F	Y	U	V	J

	T	B	O	U	F	W	K	M	H	V	A	R	X	L	N	R	W	Z	E	A	G.
Ø:	G	Y	L	F	U	D	P	N	S	E	Z	I	C	O	M	I	D	A	V	Z	T
4:	K	C	P	J	Y	H	T	R	W	I	D	M	G	S	Q	M	H	E	Z	D	X
6:	M	E	R	L	A	J	V	T	Y	K	F	O	I	U	S	O	J	G	B	F	Z
10:	Q	I	V	P	E	N	Z	X	C	O	J	S	M	Y	W	S	N	K	F	J	D

We note quickly that three Z's fall in the last three columns, strong confirmation that the four numbers of the keying sequence selected are correct.

Plaintext words are searched for between successive Z's. It is not too difficult. Here and there words appear; and finally the entire plaintext becomes evident:

TO GENERAL SMITH SIX WOUNDED FOUR KILLED TWO MISSING

With the plaintext now known, the keying sequence can be recovered:

Ciphertext:	Q	P	G	D	V	W	V	I	J	O	K	H	T	B	K	S	G	L	X
Plaintext:	T	O	Z	G	E	N	E	R	A	L	Z	S	M	I	T	H	Z	S	I
Key:	10	4	6	10	Ø	10	Ø	Ø	10	Ø	10	Ø	6	10	4	Ø	6	4	6

M	A	N	V	F	W	W	Z	C	A	E	L	P	O	A	T	B	O	U
X	Z	W	O	U	N	D	E	D	Z	F	O	U	R	Z	K	I	L	L
10	Ø	10	10	Ø	10	Ø	4	6	Ø	10	Ø	10	6	Ø	4	10	Ø	6

F	W	K	M	H	V	A	R	X	L	N	R	W	Z	E	A	G.
E	D	Z	T	W	O	Z	M	I	S	S	I	N	G	Z	Z	Z
10	Ø	10	6	4	10	Ø	4	6	4	6	Ø	10	6	4	Ø	6

With the keying sequence now recovered, the final step is to determine the "pin settings" of the two HAGELIN CRYPTOGRAPH wheels which generated the keying sequence; and at the same time to determine the lengths of the two wheels involved.

With the four numbers of the keying sequence being Ø, 4, 6, and 10. we know:

(1) that when a Ø results, the positions of both wheels are in a non-effective position.

(2) that when a 4 results, the position of the wheel containing four "lugs" is effective, and the other wheel (with its six "lugs") is non-effective.

(3) that when a 6 results, the position of the wheel containing six "lugs" is effective, and the other wheel (with four "lugs") is non-effective.

(4) that when a 10 results, the positions, or "pins", of both wheels are effective.

Therefore, "pin-settings" on the two wheels are determined to be the following:

Key:	10	4	6	10	Ø	10	Ø	Ø	10	Ø	10	Ø	6	10	4	Ø	6	4	6	10
Wheel #1:	6	Ø	6	6	Ø	6	Ø	Ø	6	Ø	6	Ø	6	6	Ø	Ø	6	Ø	6	6
Wheel #2:	4	4	Ø	4	Ø	4	Ø	Ø	4	Ø	4	Ø	Ø	4	4	Ø	Ø	4	Ø	4

Ø	10	10	Ø	10	Ø	4	6	Ø	10	Ø	10	6	Ø	4	10	Ø	6	10	Ø
Ø	6	6	Ø	6	Ø	Ø	6	Ø	6	Ø	6	6	Ø	Ø	6	Ø	6	6	Ø
Ø	4	4	Ø	4	Ø	4	Ø	Ø	4	Ø	4	Ø	Ø	4	4	Ø	Ø	4	Ø

10	6	4	10	Ø	4	6	4	6	Ø	10	6	4	Ø	6
6	6	Ø	6	Ø	Ø	6	Ø	6	Ø	6	6	Ø	Ø	6
4	Ø	4	4	Ø	4	Ø	4	Ø	Ø	4	Ø	4	Ø	Ø

Examination of the "pin settings" determined for the two wheels reveals that Wheel #1 is repeating every 19 letters and Wheel #2 is repeating every 21 letters. Thus, the two wheels and their individual keying sequences are as follows:

Wheel #1: 6 0 6 6 0 6 0 0 6 0 6 0 6 6 0 0 6 0 6

Wheel #2: 4 4 0 4 0 4 0 0 4 0 4 0 0 4 4 0 0 4 0 4 0

Before departing from this Chapter's analysis of the two-wheel HAGELIN CRYPTOGRAPH system, it might now be an appropriate time to introduce to the student one additional element or "complication" which the HAGELIN CRYPTOGRAPH's inventor has added to the basic system already discussed. This additional element or "complication" is known as the overlap, an element which adds an additional degree of security to the basic HAGELIN CRYPTOGRAPH system.

Let us, therefore, take a look at the function of the overlap. Essentially, where an overlap of "lug settings" exists between two wheels, when both wheels are effective (due to their respective "pin settings"), the effective sum of the "lugs" from each wheel is reduced by the amount of the overlap. Translated, this means that in the above cryptogram, for example, where Wheel #1 had six "lugs" and Wheel #2 had four "lugs", if there were an overlap of one "lug" between the two wheels, with both wheels effective the sum of the

"lugs" between the two wheels would not be 10, but rather 9. If the overlap were two "lugs", the effective sum of the two wheels would be 8, etc.

In other words, an overlap serves to reduce the otherwise arithmetical summation of "lugs" from two wheels by the amount of overlap.

In the HAGELIN CRYPTOGRAPH, therefore, overlaps between wheels are a good possibility; and in the two-wheel HAGELIN CRYPTOGRAPH system, the resultant key would then be Ø, $\underline{x}$, $\underline{y}$, and $\underline{z}$, where either $\underline{z} = \underline{x} + \underline{y}$ or $\underline{z}$ is less than $\underline{x} + \underline{y}$.

In the problems that follow, in this and succeeding chapters, except when otherwise indicated, use of overlaps in cryptograms should generally be expected.

PROBLEMS

21. Message begins: "REPORT FROM".

M F K L M   Q K I I Z   N A V J H   L W A O Y   N K G Z Y
F V M O R   Q G B L D   Q V R E J   M Z R L K   B L K R Q
Q J W W F   Q D A Q P   E D F U C   W S D D K.

22. Probable word: "BATTALION".

V H V W A   M I N R Y   T G N R A   O H Z E S   M M E R O
W M Y L G   M G U R R   T G K B H   I L C X L   M D H A J
Y U O G E   R T M D M   M V G R R   I M V A B   R I M O G
B O S T M   S V I H G.

23. Message begins: "TO CHIEF".

G T E F Y   R Z U G L   N Q O O F   A P V F K   X P S G H
Z E N G Z   U O E Q V   D W I N T   I D I Z R   N L Q Z O
R L Q A G.

24. Message begins: "CHANGE".

I X G M A   A L W A I   M H Q U L   C P G R L   S Y P K K
D W I A O   B S R V Y.

25. V P L X W   R C K Q H   V X X A A   Y F V I Z   T E F G I
W K P G K   H E P U A   I M V E V   M A X K V   L A O S E
V S O Q X   V H P E L.

26. Lug-settings and pin-settings of the two-wheel HAGELIN CRYPTOGRAPH used to encipher the following messages are the same. Only the "starting points" or wheel-settings are different. Further, the text of both messages is the same.

No. 1 - R A O L I P F F T L R E E M N A E I S F D L A H I
A B Y Z A.

No. 2 - I E K Q M L A O P Q Q A D N R R N D T E E G J D M
W W C V F.

27. Message begins: "TO".

G N H B V Q H H T A G O C W O X H G N H Q Z G P C
S W H Z A I G R Z B I A V L J Z T P C H M M K U K
N A M R X V C F X A I E G T O I A O C C G U N U I
R L M H A.

28. Lug-settings and pin-settings used to encipher the following two messages are the same, but the messages have different wheel-settings or "starting points" on the generated keying sequence.

No. 1 - X Y E K A D Z U N D A W Q N D Z W Z J A R B I A D.
No. 2 - S A Y P A I P D W Q L Z F G Q L U D F I.

29. I Z J R R H T V U H M T I A H P R U A G M H W G U
Y I D C G A I Y V Z N R Z D R E F G C N H B M I N
H H X H N I I G V V G N X T T G N R H J V U G G H.

30. N V A X K M V X Q A D O D N L A I L K F N X N X M
F X A I A V B I I N C U X M R Z G D C F R Q S R O
I I L V W G J W L F S I U T H I J K H T T U X E C
A Z S N L O I I C I.

Chapter 4

ANALYSIS OF A THREE-WHEEL HAGELIN CRYPTOGRAPH

In this chapter we continue our methodology of the HAGELIN CRYPTOGRAPH by analyzing the three-wheel HAGELIN CRYPTOGRAPH system. The student who by this time has a good understanding of the material presented in the first three chapters, and who hopefully has solved most of the problems presented, should have a good foundation for the progressively more difficult material of the present chapter.

Eventually we shall analyze the HAGELIN CRYPTOGRAPH with six wheels. Meanwhile, the analysis of a three-wheel machine begins to approximate the final problem.

Consider the following three-wheel problem where let us say the wheel lengths are known to be 17, 19, and 21. Let us say, too, that we know that the cryptogram begins with a stereotype beginning, the word "MESSAGE" followed by a number.

```
U B I M G   Z V M H Z   H O A H M   L A T H Z   T V B I H
H A R Q A   I M R S Z   P M S C F   L H H B Z   N N B Q B
G T S Q V   T B H G H.
```

The first step, obviously, is to recover that portion of the keying sequence where the word "MESSAGE" is set against the message beginning:

plaintext:	m	e	s	s	a	g	e	z
ciphertext:	U	B	I	M	G	Z	V	M
key:	7	6	1	5	7	6	Ø	12

We might also examine the last group of the message, hoping that the letter Z has been used as a <u>null</u> to complete the group:

plaintext:	-	z	z	z	z
ciphertext:	T	B	H	G	H
key:	-	1	7	6	7

The numbers recovered so far look extremely good. Indeed, it appears that they all could have been generated from the numbers Ø, 1, 5, and 7. That is, the numbers could have been generated from the numbers Ø 1 on one wheel, Ø 5 on another wheel, and Ø 7 on the third wheel. Thus, the

three wheels, Ø 1, Ø 5, and Ø 7, are capable of interacting (combining) in eight possible ways to generate eight possible different numbers:

Wheel #1:	Ø	Ø	Ø	Ø	1	1	1	1
Wheel #2:	Ø	5	Ø	5	Ø	5	Ø	5
Wheel #3:	Ø	Ø	7	7	Ø	Ø	7	7
Generated key:	Ø	5	7	12	1	6	8	13

Note, however, that the above different possible generated keys are those obtained <u>without overlaps</u> between wheels. If an overlap of one "lug" exists between Wheel #2 and Wheel #3, the effect of 5 + 7 would be 11, rather than 12; and thus, Ø + 5 + 7 would = 11, and 1 + 5 + 7 would = 12. Similarly, an overlap of two "lugs" between Wheel #2 and Wheel #3 would make 5 + 7 = 10; and thus, Ø + 5 + 7 would then = 10, and 1 + 5 + 7 would = 11.

It appears, therefore, that from the information available to this point the different possible generated numbers of the keying sequence, <u>with or without overlaps</u>, must be eight of the following nine:

Ø 1 5 6 7 8 11 12 13

With this knowledge, let us look for the second word of the cryptogram's text which we know from the message's stereotype beginning to be a number:

	m	e	s	s	a	g	e	z										
Ciphertext:	U	B	I	M	G	Z	V	M	H	Z	H	O	A	H	M	L	A	T
								(Ø -	s	a	s	l	z	s	n	o	z	g
								(1 -	t	b	t	m	a	t	o	p	a	h
Plaintext								(5 -	x	f	x	q	e	x	s	t	e	l
from								(6 -	y	g	y	r	f	y	t	u	f	m
possible								(7 -	z	h	z	s	g	z	u	v	g	n
keys								(8 -	a	i	a	t	h	a	v	w	h	o
								(11-	d	l	d	w	k	d	y	z	k	r
								(12-	e	m	e	x	l	e	z	a	l	s
								(13-	f	n	f	y	m	f	a	b	m	t

The problem essentially is to find which one of the following numbers fits the above possibilities:

o n e z	t e n z	n i n e t e e n z
t w o z	e l e v e n z	t w e n t y z
t h r e e z	t w e l v e z	t h i r t y z
f o u r z	t h i r t e e n z	f o r t y z
f i v e z	f o u r t e e n z	f i f t y z
s i x z	f i f t e e n z	s i x t y z
s e v e n z	s i x t e e n z	s e v e n t y z
e i g h t z	s e v e n t e e n z	e i g h t y z
n i n e z	e i g h t e e n z	n i n t y z

One by one the various numbers are tested. For example, the first number is "o n e z". Since the first ciphertext letter, H, cannot give rise to a plaintext letter "o" with any of the possible keys, the number "o n e z" is an impossibility and may be discarded. After testing each of the possible numbers, it is found that only two are possible:

(1)

Plain:	f	i	f	t	e	e	n	z
Cipher:	H	Z	H	O	A	H	M	L
Key:	13	8	13	8	5	12	Ø	11

(2)

Plain:	s	i	x	t	e	e	n	z
Cipher:	H	Z	H	O	A	H	M	L
Key:	Ø	8	5	8	5	12	Ø	11

We have already identified six numbers of the keying sequence, Ø, 1, 5, 6, 7, and 12, by setting the word "MESSAGE" against the message beginning. As a keying sequence generated from three wheels will consist of a maximum of eight different numbers, two numbers remain to be identified. But possibility (1) above adds three additional numbers, 8, 11, and 13, to the already identified six. Possibility (1), therefore, is an impossibility; and the plaintext number "s i x t e e n z" is left as the only possible number to follow the word "MESSAGE" in the cryptogram.

With the additional two numbers, 8 and 11, picked up from the word "s i x t e e n z", the eight numbers comprising the keying sequence are:

Ø 1 5 6 7 8 11 12

Having already decided that the numbers of the generated key have probably come from the numbers Ø 1 on one wheel, Ø 5 on another wheel, and Ø 7 on the third wheel, with the eight numbers making up the keying sequence being Ø 1 5 6 7 8 11 12, what can we say about overlaps?

It appears that there is an overlap of one "lug" between the wheel with five "lugs" and the wheel with seven "lugs"; thus, 5 + 7 = 11 and 1 + 5 + 7 = 12, fitting perfectly the actual generated key.

We can indicate the lug-setting with its overlap in the following fashion:

$$1 \qquad \overbrace{5 \qquad 7}^{1}$$

Up to this point with respect to the solution of the given three-wheel cryptogram, we know:

(1) The lengths of the three wheels, 17, 19, and 21.

(2) The lug-settings are 1, 5, and 7, with an <u>overlap</u> of one "lug" between the wheels with five and seven "lugs".

(3) The keying sequence for the first 16 letters and last three letters of the message.

In order to complete solution we must still:

(1) Determine to which wheels the known lug-settings apply.

(2) Determine the pin-settings of the three wheels.

(3) Read the text of the cryptogram.

To continue, let us "lay out" the message in the following manner:

Plaintext:	m	e	s	s	a	g	e	z	s	i	x	t	e	e	n	z		
Ciphertext:	U	B	I	M	G	Z	V	M	H	Z	H	O	A	H	M	L	A	T
Recovered key:	7	6	1	5	7	6	Ø	12	Ø	8	5	8	5	12	Ø	11		
Wheel Length 17:																		
Wheel Length 19:																		
Wheel Length 21:																		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

H	Z	T	V	B	I	H	H	A	R	Q	A	I	M	R	S	Z	P	M	S	C	F	L
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41

																z	z	z
H	H	B	Z	N	N	B	Q	B	G	T	S	Q	V	T	B	H	G	H
																7	6	7
42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60

Note that the lengths of the wheels, above, are repetitively indicated. It can be seen, for example, that cryptogram letters in positions 1, 18, 35, and 52 have been enciphered with key generated with the same pin of Wheel Length 17.

Looking especially at that part of the cryptogram's text where we have recovered key, it is noted that letters in positions 1-3 and 58-60 of the cryptogram have been enciphered with the same pins of Wheel Length 19.

Position 3, with its key of 1, and position 60, with its key of 7, provide the evidence that Wheel Length 19 must contain five "lugs". The reasoning is as follows:

(1) Position 3 and position 60 of Wheel Length 19 are enciphered with the same pin of Wheel Length 19; that is, there is a multiple of 19 positions between positions 3 and 60.

(2) The pin of Wheel Length 19 in positions 3 and 60 must be in a negative or non-effective position, since an effective or positive pin could not contribute to both a 1 and 7 generated key; that is, keys of 1 and 7 can only arise from two different single effective wheels, in one case a single wheel with one "lug" and in the other case a different single wheel with seven "lugs".

(3) With the pin of Wheel Length 19 non-effective in position 3, then in position 3 either Wheel Length 17 or Wheel Length 21, but not both, must be effective with one "lug" in order to give rise to the key of 1 in that position.

(4) And vice-versa, in position 60 either Wheel Length 17 or Wheel Length 21, but not both, must be effective with seven "lugs" to give rise to the key of 7 in that position.

(5) Thus, with lug totals of one and seven divided between Wheel Lengths 17 and 21, Wheel Length 19 must contain five "lugs".

We can follow the same general line of reasoning to determine the number of "lugs" on Wheel Lengths 17 and 21:

(1) Positions 7 and 58 are enciphered with the same pin of Wheel Length 17.

(2) The pin of Wheel Length 17 in positions 7 and 58 must be non-effective, since the total generated key in position 7 is Ø.

(3) Since the pin of Wheel Length 17 in position 58 must likewise be non-effective, as Wheel Length 19 is known to have five "lugs". the resultant key of 7 in position 58 can only have come from Wheel Length 21 being effective in that position with seven "lugs".

(4) With Wheel Length 19 having five "lugs", and with Wheel Length 21 having seven "lugs", Wheel Length 17 must contain one "lug".

Thus, with the number of "lugs" on each wheel known, the "effectiveness" of the pins of recovered generated key can be determined

as follows:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Plaintext:	m	e	s	s	a	g	e	z	s	i	x	t	e	e	n	z		
Ciphertext:	U	B	I	M	G	Z	V	M	H	Z	H	O	A	H	M	L	A	T
Recovered key:	7	6	1	5	7	6	Ø	12	Ø	8	5	8	5	12	Ø	11		
Wheel Length 17:	Ø	1	1	Ø	Ø	1	Ø	1	Ø	1	Ø	1	Ø	1	Ø	Ø		
Wheel Length 19:	Ø	5	Ø	5	Ø	5	Ø	5	Ø	Ø	5	Ø	5	5	Ø	5		
Wheel Length 21:	7	Ø	Ø	Ø	7	Ø	Ø	7	Ø	7	Ø	7	Ø	7	Ø	7		

19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
H	Z	T	V	B	I	H	H	A	R	Q	A	I	M	R	S	Z	P	M	S	C	F	L

42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
H	H	B	Z	N	N	B	Q	B	G	T	S	Q	V	T	B	H	G	H
																7	6	7
																Ø	1	Ø
																Ø	5	Ø
																7	Ø	7

Note, for example, that in position 1 where the generated key is 7, such a key can only arise if the pin of Wheel Length 21, with seven "lugs" thereon, is effective and the pins of the remaining two wheels are non-effective. Similarly, other generated keys can only arise if a certain wheel or wheels are effective and other wheels non-effective, etc. Remember, too, the effect of the overlap of one "lug" between Wheel Lengths 19 and 21. If both wheels are effective, their joint effectiveness is 11, i.e., 5 + 7 = 11, not 12. Thus, where the pins of all three wheels are effective, the resulting generated key will be 1 + 5 + 7 = 12.

With the "effectiveness" of pins determined for those positions of the message where key has been recovered, the now determined pins may be "marked" or indicated throughout the message as follows:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Plaintext:	m	e	s	s	a	g	e	z	s	i	x	t	e	e	n	z		
Ciphertext:	U	B	I	M	G	Z	V	M	H	Z	H	O	A	H	M	L	A	T
Recovered key:	7	6	1	5	7	6	Ø	12	Ø	8	5	8	5	12	Ø	11		
Wheel Length 17:	Ø	1	1	Ø	Ø	1	Ø	1	Ø	1	Ø	1	Ø	1	Ø	Ø		Ø
Wheel Length 19:	Ø	5	Ø	5	Ø	5	Ø	5	Ø	Ø	5	Ø	5	5	Ø	5		
Wheel Length 21:	7	Ø	Ø	Ø	7	Ø	Ø	7	Ø	7	Ø	7	Ø	7	Ø	7		

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
	H	Z	T	V	B	I	H	H	A	R	Q	A	I	M	R	S	Z	P	M	S	C	F	L
	1	1	Ø	Ø	1	Ø	1	Ø	1	Ø	1	Ø	1	Ø	Ø		Ø	1	1	Ø	Ø	1	Ø
		Ø	5	Ø	5	Ø	5	Ø	5	Ø	Ø	5	Ø	5	5	Ø	5				Ø	5	Ø
				7	Ø	Ø	Ø	7	Ø	Ø	7	Ø	7	Ø	7	Ø	7	Ø	7				

	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
																	z	z	z
	H	H	B	Z	N	N	B	Q	B	G	T	S	Q	V	T	B	H	G	H
																	7	6	7
	1	Ø	1	Ø	1	Ø	1	Ø	Ø		Ø	1	1	Ø	Ø	1	Ø	1	Ø
	5	Ø	5	Ø	5	Ø	Ø	5	Ø	5	5	Ø	5				Ø	5	Ø
		7	Ø	Ø	Ø	7	Ø	Ø	7	Ø	7	Ø	7	Ø	7	Ø	7		

At this point, identified pins fill most of the "spaces" in the message displayed above; and from these identified pins many additional keys are capable of being recovered, for example, positions 22 thru 33. For the analyst, solution at this point is all but complete -- and it is left to the student to complete if he desires.

In the problems that follow, the student will be able to test and improve his own skill in recovering key, identifying various lug-settings of wheels, identifying pin-settings, etc.

PROBLEMS

31. Wheel-Lengths: 17, 19, 21; Message begins: "FIRST"; Probable word: "ENEMY".

CUQMQ CXORG XWZAC SWHYU FYDHW
UJVWI BNUJA IYRZA GGHST HCQXT
IIQBF OYPYQ JGRZO TASLM OFWXG
LCNTW TLIGV KDZLM TJLCY UDCFH.

32. Wheel-Lengths: 26,25, 23; Probable message beginning: "REQUEST".

K A U K G H N L E T L C T Z I P K P J M T P U P N

J Y W U V H W K N E V K P V B I P G L G H J Z Z E

G F Z M O V S P H J I C U R Q R T C F H.

33. Wheel-Lengths: 23, 21, 19; Probable word: "ENEMY".

V O J I A R L S G K L A E Y Q E Q G H Z S N X E K

J Y Z R G K L E A I Y B A E D M K Q R F G A R S G

P F V T D F O K H E A N U M C B H F D E.

34. Wheel-Lengths: 21, 19, 17; Probable word: "CONTINUE".

J L O B V O A A P W F M E E W Y E E X Z T D K J I

C A I L M Y G E M L J F L K M P U R M T V O E F H

S D U M G K G P R N O L F M A U S Y M R.

35. Wheel-Lengths: 23, 21, 19; Both messages contain same plaintext, but have been enciphered with different "wheel settings".

No. 1 - I T N Y Y T F Y F R W G P L D G Y C V L I J M A J

P R Q L M F W L R K K R H L A C X H A I.

No. 2 - F L Y Q C U A A H S V C X A R Z W A D F N E H K E

R S I T O V H D Z C S N I I C D W A I H.

36. Wheel-Lengths: 21, 19, 17; All messages have been enciphered with the same initial "wheel settings".

No. 1 - Z R U K N I F E N O J T Z L W F G Y O A D N Y G C

Z I Q Q N R P Y E F U R Z Y U F S G I K.

No. 2 - L L M A Z Z C Z H P P P S O L F A C M S Y N D T A

C E K Z B Z V B D C G H Y T D L N N N W W Q W V R.

No. 3 - A M H Q I I Y M H P Q W W O K I C Y G D P Y D B Q

P I S A B R J L L C C N Y Y J T A X D J M F F E W

X V H F D.

No. 4 - X Z Q Y H Q C E E A F B I K V W P N A T U H D U W

V D R F R Q U G V F F I U I W H A A I K.

No. 5 - I V M P C D D F Z D Y P I A K.

37. Wheel-Lengths 23, 21, 19; Message beginning: "ENEMY".

X M A S G C O C O X H C P R Z S J X E A X P A G E

X R A G A M L L P C S Z L I Q T M A B L D G B B R

P Z A H E M O C L I M A F F D.

38. Wheel-Lengths 21, 19, 17; Message begins "RADIO TRANSMISSIONS".

T Z G C T   L Q N Z R   R Q W R H   C O R H K   C T W Q L
H Q Q Y K   G D U V N   N A Z X F   J W V K K   A D Y S E
A K L F F   L A G X H   K P G L F   P N F E Z   G D Z D D.

39. Wheel-Lengths 26, 25, 23; Message begins with word "MESSAGE" followed by a number.

A B R N M   J V L B Q   Y G M A H   B P C L C   A I P N B
B L V F V   P C W B A   Q O Z F E   E C N D V   C C A K F
T H N I G   C I B Y G   M M Q Z E   H D S Q P   U R A K Q
Z L M I W   O L G N F.

40. Wheel-Lengths 26, 24, 17; Messages have been enciphered with different "wheel settings".

No. 1 - A V B B Q   A T G A Z   M A J O J   Q U T N K   B G P L J.
No. 2 - P W J X M   R K Z P K   B R A G H   L C G G L   P G N G H
K R M V O   R D L E N   Y X L G F   T P A L S   J O X R S
V G M F P   L O O L L   X J G F P.

Chapter 5

ANALYSIS OF A FOUR-WHEEL HAGELIN CRYPTOGRAPH

In this chapter we have reached another "stepping stone" in our study of the cryptanalysis of the HAGELIN CRYPTOGRAPH. Having studied the analysis of the HAGELIN CRYPTOGRAPH in some detail up to the three-wheel system, we are ready now to turn to the next progressively more difficult system, that of the four-wheel HAGELIN CRYPTOGRAPH.

Therefore, let us turn our attention now to the solution of a HAGELIN cryptogram, enciphered with four wheels of lengths 17, 19, 21, and 23. Further, in order to introduce the student to an important "general method" to solve the HAGELIN CRYPTOGRAPH, we shall use this method to solve the cryptogram given. This method is particularly important because it is based upon "frequency considerations" of plaintext, rather than upon knowledge of a stereotype message beginning, probable words, etc.; and of course, too, the student should keep in mind that though in this case we are dealing with a four-wheel HAGELIN system, the same "principles" generally hold true for the ultimate six-wheel HAGELIN CRYPTOGRAPH.

The cryptogram:

```
N G A P Y   Z A T P X   H C I R F   S P B K M   F J R M H
J O F C N   J E V V O   Q D M W E   T Q P V Q   T B Q I M
L G O M J   H D A U G   V I A X V   N H K W H   O B E S V
B I Q I E   N I X A T   C H H R D   R L G V M   X X J N M
G U A B D   V I H B R   D M B N D   R M F A W   X V I Z V

O C F I M   L X S Q O   P Q U X D   K W V W I   R R R A C
L O W A R   P X B A T   Y B D T Z   J F A T R   X V D Z K
I M O N N   X Y P U R   Z W G L R   C S B R M   L W I T J
F R O K A   X D K Q A   S D H X U   T W B W J   N Q A Y A
F B H Q P   D P S F G   S H Q H A   O I D N J   F G Z D T

Y U D A J   F A R L Z   P W L H N   I Q I H I   O Q J N F
C M G Q L   D J C E O   O P Y Q R   U P R L V   V Q K Y D
H J N S E   Q F Y X D   L E V K J   M Q O E B   C O J G M
I T Y I P   H P N O F   C P N V I   A K U J R   H X U M M
O P B G N   Y Z X A P   M X V F W   G I C G N   J I V X A
```

MEMQW YFBRH DAVEJ ERVSY VALWX
SJLPR WAAOL LLHPY LVYIL UKOBZ
MKUYD HHJID DZTAZ TGKQH ARHLQ
FYEYV TMHPI WYOJQ UMDSX LSBWK
NKIUL WKJYH SNMNH ICJNL MFDFJ

URDQS PZYJE UNWLU GSMID XYDYJ
LIPVX ITSKB VDCDN MYBCP UNXRZ
QVZBK YLAJC XRABX VXFVD MJUYU
UAOUE QOUAG JRTQD SDEDA MKNPV
LBVDP MYHTA QHBZV YNBMV KBYNM

JLRIT WYEMR CAQAI ROJTM BPDIV
JQUAG LSVVL UOJMW RLMWJ DUUKI
NOAMC HPTNS ELLJE OLFKI OBIGK
RTRBJ USHUF AYBBA SDVJB VYQDQ
ECJCA FEKTZ MAHEI DDSHP CXBGV

HLMLD EGTME ZLIBN VPDND.

It is noted that the cryptogram is fairly lengthy, 770 letters in length; or, assuming six letters per word, the cryptogram is about 128 words long.

Let us begin our analysis by writing the cryptogram horizontally with a "period" of 17, to produce 17 columns. Each column will then represent those letters enciphered with the same pin-setting of Wheel Length 17.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
N	G	A	P	Y	Z	A	T	P	X	H	C	I	R	F	S	P
B	K	M	F	J	R	M	H	J	O	F	C	N	J	E	V	V
O	Q	D	M	W	E	T	Q	P	V	Q	T	B	Q	I	M	L
G	O	M	J	H	D	A	U	G	V	I	A	X	V	N	H	K
W	H	O	B	E	S	V	B	I	Q	I	E	N	I	X	A	T
C	H	H	R	D	R	L	G	V	M	X	X	J	N	M	G	U
A	B	D	V	I	H	B	R	D	M	B	N	D	R	M	F	A
W	X	V	I	Z	V	O	C	F	I	M	L	X	S	Q	O	P
Q	U	X	D	K	W	V	W	I	R	R	R	A	C	L	O	W
A	R	P	X	B	A	T	Y	B	D	T	Z	J	F	A	T	R
X	V	D	Z	K	I	M	O	N	N	X	Y	P	U	R	Z	W
G	L	R	C	S	B	R	M	L	W	I	T	J	F	R	O	K
A	X	D	K	Q	A	S	D	H	X	U	T	W	B	W	J	N

Q	A	Y	A	F	B	H	Q	P	D	P	S	F	G	S	H	Q
H	A	O	I	D	N	J	F	G	Z	D	T	Y	U	D	A	J
F	A	R	L	Z	P	W	L	H	N	I	Q	I	H	I	O	Q
J	N	F	C	M	G	Q	L	D	J	C	E	O	O	P	Y	Q
R	U	P	R	L	V	V	Q	K	Y	D	H	J	N	S	E	Q
F	Y	X	D	L	E	V	K	J	M	Q	O	E	B	C	O	J
G	M	I	T	Y	I	P	H	P	N	O	F	C	P	N	V	I
A	K	U	J	R	H	X	U	M	M	O	P	B	G	N	Y	Z
X	A	P	M	X	V	F	W	G	I	C	G	N	J	I	V	X
A	M	E	M	Q	W	Y	F	B	R	H	D	A	V	E	J	E
R	V	S	Y	V	A	L	W	X	S	J	L	P	R	W	A	A
O	L	L	L	H	P	Y	L	V	Y	I	L	U	K	O	B	Z
M	K	U	Y	D	H	H	J	I	D	D	Z	T	A	Z	T	G
K	Q	H	A	R	H	L	Q	F	Y	E	Y	V	T	M	H	P
I	W	Y	O	J	Q	U	M	D	S	X	L	S	B	W	K	N
K	I	U	L	W	K	J	Y	H	S	N	M	N	H	I	C	J
N	L	M	F	D	F	J	U	R	D	Q	S	P	Z	Y	J	E
U	N	W	L	U	G	S	M	I	D	X	Y	D	Y	J	L	I
P	V	X	I	T	S	K	B	V	D	C	D	N	M	Y	B	C
P	U	N	X	R	Z	Q	V	Z	B	K	Y	L	A	J	C	X
R	A	B	X	V	X	F	V	D	M	J	U	Y	U	U	A	O
U	E	Q	O	U	A	G	J	R	T	Q	D	S	D	E	D	A
M	K	N	P	V	L	B	V	D	P	M	Y	H	T	A	Q	H
B	Z	V	Y	N	B	M	V	K	B	Y	N	M	J	L	R	I
T	W	Y	E	M	R	C	A	Q	A	I	R	O	J	T	M	B
P	D	I	V	J	Q	U	A	G	L	S	V	V	L	U	O	J
M	W	R	L	M	W	J	D	U	U	K	I	N	O	A	M	C
H	P	T	N	S	E	L	L	J	E	O	L	F	K	I	O	B
I	G	K	R	T	R	B	J	U	S	H	U	F	A	Y	B	B
A	S	D	V	J	B	V	Y	Q	D	Q	E	C	J	C	A	F
E	K	T	Z	M	A	H	E	I	D	D	S	H	P	C	X	B
G	V	H	L	M	L	D	E	G	T	M	E	Z	L	I	B	N
V	P	D	N	D.												

Each column represents letters similarly enciphered with a given pin-setting on Wheel Length 17 -- the pin being either "effective" or "non-effective". Thus, the 17 columns in effect represent two classes of columns, those columns with "effective" pins on Wheel Length 17 and those columns with "non-effective" pins on Wheel Length 17.

The student will remember that --

(1) encipherment with a single-wheel of the HAGELIN CRYPTOGRAPH results in encipherment with two Beaufort cipher alphabets; that is, a single wheel results in two numbers of "key", one of the numbers being Ø.

(2) encipherment with two-wheels of the HAGELIN CRYPTOGRAPH results in an encipherment with four Beaufort cipher alphabets; that is, two wheels result in four numbers of "key", one of the four being Ø.

(3) encipherment with three-wheels of the HAGELIN CRYPTOGRAPH

results in an encipherment with eight Beaufort cipher alphabets; that is, three wheels result in eight numbers of "key", one of the numbers being Ø.

Therefore, consider the 17 columns, above, which as we noted are divided into two classes, those columns with "effective" pins on Wheel Length 17 and those columns with "non-effective" pins on Wheel Length 17. We may make the following important observations --

(1) Letters within columns where the pins of Wheel Length 17 are "non-effective" are enciphered as the result of the other three wheels generating eight Beaufort cipher alphabets. For these letters it is just as if Wheel Length 17 did not exist.

(2) Letters within columns, on the other hand, where the pins of Wheel Length 17 are "effective" are enciphered as the result of the generation of eight other Beaufort cipher alphabets by the other three wheels plus the constant "effectiveness" of Wheel Length 17.

Thus, encipherment with four wheels of the HAGELIN CRYPTOGRAPH results in encipherment with 16 Beaufort cipher alphabets, eight Beaufort cipher alphabets produced by a "non-effective" pin on Wheel Length 17 and eight other Beaufort cipher alphabets produced by an "effective" pin on Wheel Length 17.

By matching frequency distributions of each of the 17 columns we shall attempt to divide the columns into their two classes. Success will depend upon whether we have a sufficient number of letters within a column to provide a differentation between polyalphabeticity with eight alphabets of one class and polyalphabeticity with a different eight alphabets of another class.

Frequency distributions of the 17 columns are as follows:

#1:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
6	2	1		1	2	4	2	2	1	2		3	2	2	3	2	3		1	2	1	2	2		

#2:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
5	1		1	1		2	2	1		5	3	2	2	1	2	2	1	1		3	4	3	2	1	1

#3:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	1		6	1	1		3	2		1	1	3	2	2	3	1	3	1	2	3	2	1	3	3	

#4:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	2	1	2	2	1	2			3	2	1	6	3	2	2	2		3		1		3		3	3	2

#5:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
		1		5	1	1		2	1	4	2	2	5	1			2	3	2	2	2	3	2	1	2	2

#6:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	5	4		1	3	1	2	4	2		1	2		1		2	2	4	2			3	3	1		2

#7:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	2	3	1	1		2	1	3		4	1	4	3		1	1	2	1	2	2	2	5	1	1	2	

#8:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	2	2	1	2	2	2	1	2		3	1	4	3		1		4	1		1	3	4	3		3	

#9:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
		2		5		2	5	3	5	3	2	1	1	1		4	2	2			2	3		1		1

#10:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	1	2		8	1				2	1		1	5	3	1	1	1	2	4	2	1	2	1	2	3	1

#11:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
		1	3	4	1	1		3	6	2	2		3	1	3	1	5	1	1	1	1			4	1	

#12:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	1		2	3	4	1	1	1	1			5	1	2	1	1	1	2	3	4	2	1		1	5	2

#13:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	2	2	2	2	1	3		2	2	4		1	1	6	2	3			2	1	1	2	1	2	2	1

#14:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	3	3	1	1		2	2	2	1	5	2	2	1	2	2	2	1	3	1	2	3	2			1	1

#15:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	3		3	1	3	1			6	2		2	3	3	1	1	1	2	2	1	2		3	1	3	1

#16:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	5	4	2	1	1	1	1	3		3	1	1	3		7		1	1	1	2		3		1	2	1

#17:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	3	4	2		2	1	1	1	3	4	2	1		3	1	3	4	1		1	1	1	2	2		2

The "cross-product sum" or Chi test, described by Dr. Solomon Kullback in his classic treatise, "Statistical Methods in Cryptanalysis", provides a method to match frequency distributions. It is assumed that the student is fully acquainted with the Chi test which is of fundamental importance in cryptanalysis.

For purpose of illustration consider the "matching" of Frequency Distribution #1 with Frequency Distribution #2:

	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency Distribution #1:	6	2	1		1	2	4	2	2	1	2		3
Frequency Distribution #2:	5	1		1	1		2	2	1		5	3	2
	30	2			1		8	4	2		10		6

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	2	2	3	2	3		1	2	1	2	2		
	2	1	2	2	1	1		3	4	3	2	1	1
	4	2	6	4	3			6	4	6	4		

$$\underline{\text{chi}}\ \text{test (\#1 and \#2)} = \frac{\text{Sum of cross-products}}{N_1 \times N_2} = \frac{102}{2116} = 0.048$$

Where: $N_1 \times N_2 = 46 \times 46 = 2116$

Sum of cross-products = 30+2+1+8+4+2+10+6+4+2+6+4+3+6+4+6+4 = 102

In likewise fashion, the chi test is made each pair of frequency distributions -- and results are as follows:

#1 + #2 = 0.048	#1 + #3 = 0.037	#1 + #4 = 0.034
#1 + #5 = 0.030	#1 + #6 = 0.048	#1 + #7 = 0.036
#1 + #8 = 0.036	#1 + #9 = 0.042	#1 + #10 = 0.030
#1 + #11 = 0.037	#1 + #12 = 0.026	#1 + #13 = 0.037
#1 + #14 = 0.043	#1 + #15 = 0.039	#1 + #16 = 0.045
#1 + #17 = 0.044		

#2 + #3 = 0.039	#2 + #4 = 0.040	#2 + #5 = 0.037
#2 + #6 = 0.048	#2 + #7 = 0.043	#2 + #8 = 0.044
#2 + #9 = 0.039	#2 + #10 = 0.034	#2 + #11 = 0.031
#2 + #12 = 0.032	#2 + #13 = 0.033	#2 + #14 = 0.039
#2 + #15 = 0.035	#2 + #16 = 0.039	#2 + #17 = 0.040

#3 + #4 = 0.042	#3 + #5 = 0.048	#3 + #6 = 0.036
#3 + #7 = 0.038	#3 + #8 = 0.039	#3 + #9 = 0.046
#3 + #10 = 0.058	#3 + #11 = 0.048	#3 + #12 = 0.043
#3 + #13 = 0.040	#3 + #14 = 0.033	#3 + #15 = 0.038
#3 + #16 = 0.036	#3 + #17 = 0.029	

#4 + #5 = 0.042	#4 + #6 = 0.036	#4 + #7 = 0.043
#4 + #8 = 0.041	#4 + #9 = 0.038	#4 + #10 = 0.044
#4 + #11 = 0.039	#4 + #12 = 0.047	#4 + #13 = 0.042
#4 + #14 = 0.039	#4 + #15 = 0.045	#4 + #16 = 0.041
#4 + #17 = 0.036		

#5 + #6 = 0.034	#5 + #7 = 0.043	#5 + #8 = 0.048
#5 + #9 = 0.043	#5 + #10 = 0.057	#5 + #11 = 0.043
#5 + #12 = 0.041	#5 + #13 = 0.036	#5 + #14 = 0.040
#5 + #15 = 0.038	#5 + #16 = 0.036	#5 + #17 = 0.031

#6 + #7 = 0.040	#6 + #8 = 0.040	#6 + #9 = 0.041
#6 + #10 = 0.033	#6 + #11 = 0.030	#6 + #12 = 0.033
#6 + #13 = 0.034	#6 + #14 = 0.040	#6 + #15 = 0.036
#6 + #16 = 0.041	#6 + #17 = 0.044	

#7 + #8 = 0.054	#7 + #9 = 0.040	#7 + #10 = 0.039
#7 + #11 = 0.033	#7 + #12 = 0.038	#7 + #13 = 0.039
#7 + #14 = 0.047	#7 + #15 = 0.031	#7 + #16 = 0.049
#7 + #17 = 0.037		

#8 + #9 = 0.037	#8 + #10 = 0.039	#8 + #11 = 0.035
#8 + #12 = 0.040	#8 + #13 = 0.034	#8 + #14 = 0.041
#8 + #15 = 0.037	#8 + #16 = 0.043	#8 + #17 = 0.037

#9 + #10 = 0.043	#9 + #11 = 0.049	#9 + #12 = 0.029
#9 + #13 = 0.039	#9 + #14 = 0.044	#9 + #15 = 0.033
#9 + #16 = 0.029	#9 + #17 = 0.041	

#10 + #11 = 0.047	#10 + #12 = 0.048	#10 + #13 = 0.043
#10 + #14 = 0.033	#10 + #15 = 0.043	#10 + #16 = 0.037
#10 + #17 = 0.028		

#11 + #12 = 0.033	#11 + #13 = 0.039	#11 + #14 = 0.033
#11 + #15 = 0.045	#11 + #16 = 0.039	#11 + #17 = 0.042

#12 + #13 = 0.037	#12 + #14 = 0.033	#12 + #15 = 0.044
#12 + #16 = 0.033	#12 + #17 = 0.027	
#13 + #14 = 0.043	#13 + #15 = 0.043	#13 + #16 = 0.040
#13 + #17 = 0.044		
#14 + #15 = 0.034	#14 + #16 = 0.046	#14 + #17 = 0.044
#15 + #16 = 0.032	#15 + #17 = 0.040	
#16 + #17 = 0.039		

The above $\frac{17(17-1)}{2}$ = 136 chi test results indicate the degree of likelihood that matched pairs of frequency distributions are from the same class of "eight-alphabet polyalphabeticity". The larger the value of the result, the more likely it is that the pairs of frequency distributions are of the same class; and conversely, the lower the value of the result, the less likely it is that the pairs are of the same class.

A tabulation of the above results shows:

(1) the three lowest results are 0.026, 0.027, and 0.028.

(2) the three largest results are 0.054, 0.057, and 0.058.

(3) the average or median result is 0.039.

Based on these results, we can say then that a result less than 0.039 is more likely to be an incorrect match, while a result larger than 0.039 is more likely to be a correct match.

Let us make the assumption that the three lowest results are a valid indication of an incorrect match; and that the three largest results are a valid indication of a correct match. We have then:

Correct match	Incorrect match
#7 + #8 = 0.054	#1 + #12 = 0.026
#5 + #10 = 0.057	#12 + #17 = 0.027
#3 + #10 = 0.058	#10 + #17 = 0.028

From these matches we can see that:

(1) #7 and #8 are in the same class.

(2) #1 and #17 are in the same class.

(3) #3, #5, #10, and #12 are in the same class.

(4) #1 and #17 are not in the same class as #3, #5, #10, and #17.

Labelling #1 and #17 as Class A, and #3, #5, #10, and #12 as Class B, let us continue by comparing Frequency Distribution #2 with these tentative classes:

Class A	Class B
#2 + #1 = 0.048	#2 + #3 = 0.039
#2 + #17 = 0.040	#2 + #5 = 0.037
	#2 + #10 = 0.034
	#2 + #12 = 0.032

From these matches or comparisons it appears Frequency Distribution #2 is clearly in Class A. Therefore, #2 may be added to #1 and #17 in Class A.

In the same manner, let us compare Frequency Distribution #4 with Classes A and B:

Class A	Class B
#4 + #1 = 0.034	#4 + #3 = 0.042
#4 + #2 = 0.040	#4 + #5 = 0.042
#4 + #17 = 0.036	#4 + #10 = 0.044
	#4 + #12 = 0.047

From these comparisons it appears that Frequency Distribution #4 is almost surely in Class B; and, therefore, #4 is added to Class B.

Again in the same manner, Frequency Distribution #6 can be compared with Classes A and B:

Class A	Class B
#6 + #1 = 0.048	#6 + #3 = 0.036
#6 + #2 = 0.048	#6 + #4 = 0.036
#6 + #17 = 0.044	#6 + #5 = 0.034
	#6 + #10 = 0.033
	#6 + #12 = 0.033

It could hardly be more clear that Frequency Distribution #6 is in Class A; and, with no hesitation #6 can be added to #1, #2, and #17 in Class A.

To continue, Frequency Distribution #14 is compared with the distributions of Classes A and B:

Class A	Class B
#14 + #1 = 0.043	#14 + #3 = 0.033
#14 + #2 = 0.039	#14 + #4 = 0.039
#14 + #6 = 0.040	#14 + #5 = 0.040
#14 + #17 = 0.044	#14 + #10 = 0.033
	#14 + #12 = 0.033

It appears clear that Frequency Distribution #14 can be added to Class A.

Continuing, Frequency Distribution #15 is matched with the distributions of Class A and B:

Class A	Class B
#15 + #1 = 0.039	#15 + #3 = 0.038
#15 + #2 = 0.035	#15 + #4 = 0.045
#15 + #6 = 0.036	#15 + #5 = 0.038
#15 + #14 = 0.034	#15 + #10 = 0.043
#15 + #17 = 0.040	#15 + #12 = 0.044

It seems evident that Frequency Distribution #15 is in Class B; and #15, therefore, is added to the distributions of Class B.

Frequency Distribution #16 is compared with the distributions of Classes A and B:

Class A	Class B
#16 + #1 = 0.045	#16 + #3 = 0.036
#16 + #2 = 0.039	#16 + #4 = 0.041
#16 + #6 = 0.041	#16 + #5 = 0.036
#16 + #14 = 0.046	#16 + #10 = 0.037
#16 + #17 = 0.039	#16 + #12 = 0.033
	#16 + #15 = 0.032

With the exception of (#16 + #4 = 0.041), Frequency Distribution #16 fits well into Class A; and, therefore, Class A gains another distribution.

Frequency Distribution #11 is compared with the distributions in the expanding Classes A and B:

Class A	Class B
#11 + #1 = 0.037	#11 + #3 = 0.048
#11 + #2 = 0.031	#11 + #4 = 0.039
#11 + #6 = 0.030	#11 + #5 = 0.043
#11 + #14 = 0.033	#11 + #10 = 0.047
#11 + #16 = 0.039	#11 + #12 = 0.033
#11 + #17 = 0.042	#11 + #15 = 0.045

Visually it can be seen that it is most probable that Frequency Distribution #11 belongs in Class B. But this comparison brings up a good point: the values derived from the chi test (or any other test) will not prove a "fact" beyond a shadow of doubt and should not be taken as positive proof. Thus, in the above comparisons, we should assume that (#11 + #17 = 0.042) and (#11 + #12 = 0.033) have simply occurred by chance; and to make a sound decision as to what Class to put Distribution #11 into depends upon how Distribution #11 compares to the distributions of Class A "as a whole" and to the distributions of Class B "as a whole".

While we could add all the frequencies of the distributions in Class A together and make a new chi test with Distribution #11 on a larger scale, and do the same for Class B, and though this would be very accurate, for our purpose here it appears fairly evident, in spite of (#11 + #17 = 0.042) and (#11 + #12 = 0.033), that Frequency Distribution #11 belongs in Class B. Indeed, another way of looking at the decision making process is to take the "average" of the chi test results of Class A, above, and compare it with the "average" of the results of Class B. It will be found that the "average" of the chi test results of Class A, above, is 0.035; and the "average" of the Class B results is 0.042. Thus, it is most probable that Frequency Distribution #11 belongs in Class B.

Let us turn now to Frequency Distributions #7 and #8, which we assumed originally, to be in the same class. Let us attempt to place these two distributions either in Class A or Class B.

We shall match, therefore, distributions #7 and #8 with the various

distributions which now comprise Class A and Class B, as follows:

Class A	Class B
#7 + #1 = 0.036	#7 + #3 = 0.038
#7 + #2 = 0.043	#7 + #4 = 0.043
#7 + #6 = 0.040	#7 + #5 = 0.043
#7 + #14 = 0.047	#7 + #10 = 0.039
#7 + #16 = 0.049	#7 + #11 = 0.033
#7 + #17 = 0.037	#7 + #12 = 0.038
	#7 + #15 = 0.031
#8 + #1 = 0.036	#8 + #3 = 0.039
#8 + #2 = 0.044	#8 + #4 = 0.041
#8 + #6 = 0.040	#8 + #5 = 0.048
#8 + #14 = 0.041	#8 + #10 = 0.039
#8 + #16 = 0.043	#8 + #11 = 0.035
#8 + #17 = 0.037	#8 + #12 = 0.040
	#8 + #15 = 0.037

It is likely that most analysts would subjectively select Class A for inclusion of Frequency Distributions #7 and #8; but taking the average of the chi test results of Class A vs. the average of the chi test results of Class B would provide a method of making purely an objective determination. Thus, the average of the Class A results is 0.041^{+} and the average of the Class B results is 0.039^{-}. It would appear that Frequency Distributions #7 and #8 do belong in Class A.

We turn now to Frequency Distribution #9. Matching Distribution #9 against the distributions of Classes A and B produces the following:

Class A	Class B
#9 + #1 = 0.042	#9 + #3 = 0.046
#9 + #2 = 0.039	#9 + #4 = 0.038
#9 + #6 = 0.041	#9 + #5 = 0.043
#9 + #7 = 0.040	#9 + #10 = 0.043
#9 + #8 = 0.037	#9 + #11 = 0.049
#9 + #14 = 0.044	#9 + #12 = 0.029
#9 + #16 = 0.029	#9 + #15 = 0.033
#9 + #17 = 0.041	

Here we indeed have a problem! But after all this is the typical HAGELIN CRYPTOGRAPH problem -- on a reduced scale, perhaps, because this is a four-wheel cryptogram. But nonetheless the inability to "clearly" put a distribution into this or that class is common, especially where the amount of text is limited. In the present case we have about 45 letters per column. With the 45 letters representing the polyalphabeticity of eight different alphabets, it is no wonder that there will be expected difficulty to successfully match all the distributions. We have two choices. We can simply make an "educated guess" as to which class the distribution belongs, or we can attempt to continue with the solution without identifying the class to which the column belongs.

In matching Frequency Distribution #9, the average chi test result of the Class A comparisons is 0.039^{+}, and the average chi test result of the Class B comparisons is 0.040^{+}. With any degree of reliability, and with the amount of text available, we cannot at this point put the distribution in either Class A or Class B. Therefore, for the moment let us leave Frequency Distribution #9 unidentified as to class.

We are left with the final distribution, Frequency Distribution #13. Matching Frequency Distribution #13 with the distributions of the Classes A and B produces the following:

Class A	Class B
#13 + #1 = 0.037	#13 + #3 = 0.040
#13 + #2 = 0.033	#13 + #4 = 0.042
#13 + #6 = 0.034	#13 + #5 = 0.036
#13 + #7 = 0.039	#13 + #10 = 0.043
#13 + #8 = 0.034	#13 + #11 = 0.039
#13 + #14 = 0.043	#13 + #12 = 0.037
#13 + #16 = 0.040	#13 + #15 = 0.043
#13 + #17 = 0.044	

Again, even visually we can quickly see that Frequency Distribution #13 does not clearly fit into either Class A or Class B. Just as we did with Distribution #9, for the moment let us leave Frequency Distribution #13 unidentified as to class.

Thus, in summary before going on to the next step in the solution of

our given cryptogram, we have up to this point divided 15 of 17 pins on Wheel Length 17 into two arbitrary classes, Class A and Class B. One of the classes represents "effective" pins and one represents "non-effective" pins. The classes are:

Class A: 1, 2, 6, 7, 8, 14, 16, and 17.

Class B: 3, 4, 5, 10, 11, 12, and 15.

Before turning to Wheel Length 19, let us once again write the cryptogram horizontally with a "period" of 17, producing 17 columns; but this time let us identify the individual letters in their columns with the small-letters "a" and "b" to indicate the class to which the letters belong.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Na	Ga	Ab	Pb	Yb	Za	Aa	Ta	P	Xb	Hb	Cb	I	Ra	Fb	Sa	Pa
Ba	Ka	Mb	Fb	Jb	Ra	Ma	Ha	J	Ob	Fb	Cb	N	Ja	Eb	Va	Va
Oa	Qa	Db	Mb	Wb	Ea	Ta	Qa	P	Vb	Qb	Tb	B	Qa	Ib	Ma	La
Ga	Oa	Mb	Jb	Hb	Da	Aa	Ua	G	Vb	Ib	Ab	X	Va	Nb	Ha	Ka
Wa	Ha	Ob	Bb	Eb	Sa	Va	Ba	I	Qb	Ib	Eb	N	Ia	Xb	Aa	Ta
Ca	Ha	Hb	Rb	Db	Ra	La	Ga	V	Mb	Xb	Xb	J	Na	Mb	Ga	Ua
Aa	Ba	Db	Vb	Ib	Ha	Ba	Ra	D	Mb	Bb	Nb	D	Ra	Mb	Fa	Aa
Wa	Xa	Vb	Ib	Zb	Va	Oa	Ca	F	Ib	Mb	Lb	X	Sa	Qb	Oa	Pa
Qa	Ua	Xb	Db	Kb	Wa	Va	Wa	I	Rb	Rb	Rb	A	Ca	Lb	Oa	Wa
Aa	Ra	Pb	Xb	Bb	Aa	Ta	Ya	B	Db	Tb	Zb	J	Fa	Ab	Ta	Ra
Xa	Va	Db	Zb	Kb	Ia	Ma	Oa	N	Nb	Xb	Yb	P	Ua	Rb	Za	Wa
Ga	La	Rb	Cb	Sb	Ba	Ra	Ma	L	Wb	Ib	Tb	J	Fa	Rb	Oa	Ka
Aa	Xa	Db	Kb	Qb	Aa	Sa	Da	H	Xb	Ub	Tb	W	Ba	Wb	Ja	Na
Qa	Aa	Yb	Ab	Fb	Ba	Ha	Qa	P	Db	Pb	Sb	F	Ga	Sb	Ha	Qa
Ha	Aa	Ob	Ib	Db	Na	Ja	Fa	G	Zb	Db	Tb	Y	Ua	Db	Aa	Ja
Fa	Aa	Rb	Lb	Zb	Pa	Wa	La	H	Nb	Ib	Qb	I	Ha	Ib	Oa	Qa
Ja	Na	Fb	Cb	Mb	Ga	Qa	La	D	Jb	Cb	Eb	O	Oa	Pb	Ya	Qa
Ra	Ua	Pb	Rb	Lb	Va	Va	Qa	K	Yb	Db	Hb	J	Na	Sb	Ea	Qa
Fa	Ya	Xb	Db	Lb	Ea	Va	Ka	J	Mb	Qb	Ob	E	Ba	Cb	Oa	Ja
Ga	Ma	Ib	Tb	Yb	Ia	Pa	Ha	P	Nb	Ob	Fb	C	Pa	Nb	Va	Ia
Aa	Ka	Ub	Jb	Rb	Ha	Xa	Ua	M	Mb	Ob	Pb	B	Ga	Nb	Ya	Za
Xa	Aa	Pb	Mb	Xb	Wa	Fa	Wa	G	Ib	Cb	Gb	N	Ja	Ib	Va	Xa
Aa	Ma	Eb	Mb	Qb	Wa	Ya	Fa	B	Rb	Hb	Db	A	Va	Eb	Ja	Ea
Ra	Va	Sb	Yb	Vb	Aa	La	Wa	X	Sb	Jb	Lb	P	Ra	Wb	Aa	Aa
Oa	La	Lb	Lb	Hb	Pa	Ya	La	V	Yb	Ib	Lb	U	Ka	Ob	Ba	Za
Ma	Ka	Ub	Yb	Db	Ha	Ha	Ja	I	Db	Db	Zb	T	Aa	Zb	Ta	Ga
Ka	Qa	Hb	Ab	Rb	Ha	La	Qa	F	Yb	Eb	Yb	V	Ta	Mb	Ha	Pa
Ia	Wa	Yb	Ob	Jb	Qa	Ua	Ma	D	Sb	Xb	Lb	S	Ba	Wb	Ka	Na
Ka	Ia	Ub	Lb	Wb	Ka	Ja	Ya	H	Sb	Nb	Mb	N	Ha	Ib	Ca	Ja
Na	La	Mb	Fb	Db	Fa	Ja	Ua	R	Db	Qb	Sb	P	Za	Yb	Ja	Ea
Ua	Na	Wb	Lb	Ub	Ga	Sa	Ma	I	Db	Xb	Yb	D	Ya	Jb	La	Ia
Pa	Va	Xb	Ib	Tb	Sa	Ka	Ba	V	Db	Cb	Db	N	Ma	Yb	Ba	Ca
Pa	Ua	Nb	Xb	Rb	Za	Qa	Va	Z	Bb	Kb	Yb	L	Aa	Jb	Ca	Xa
Ra	Aa	Bb	Xb	Vb	Xa	Fa	Va	D	Mb	Jb	Ub	Y	Ua	Ub	Aa	Oa
Ua	Ea	Qb	Ob	Ub	Aa	Ga	Ja	R	Tb	Qb	Db	S	Da	Eb	Da	Aa
Ma	Ka	Nb	Pb	Vb	La	Ba	Va	D	Pb	Mb	Yb	H	Ta	Ab	Qa	Ha

Ba	Za	Vb	Yb	Nb	Ba	Ma	Va	K	Bb	Yb	Nb	M	Ja	Lb	Ra	Ia
Ta	Wa	Yb	Eb	Mb	Ra	Ca	Aa	Q	Ab	Ib	Rb	O	Ja	Tb	Ma	Ba
Pa	Da	Ib	Vb	Jb	Qa	Ua	Aa	G	Lb	Sb	Vb	V	La	Ub	Oa	Ja
Ma	Wa	Rb	Lb	Mb	Wa	Ja	Da	U	Ub	Kb	Ib	N	Oa	Ab	Ma	Ca
Ha	Pa	Tb	Nb	Sb	Ea	La	La	J	Eb	Ob	Lb	F	Ka	Ib	Oa	Ba
Ia	Ga	Kb	Rb	Tb	Ra	Ba	Ja	U	Sb	Hb	Ub	F	Aa	Yb	Ba	Ba
Aa	Sa	Db	Vb	Jb	Ba	Va	Ya	Q	Db	Qb	Eb	C	Ja	Cb	Aa	Fa
Ea	Ka	Tb	Zb	Mb	Aa	Ha	Ea	I	Db	Db	Sb	H	Pa	Cb	Xa	Ba
Ga	Va	Hb	Lb	Mb	La	Da	Ea	G	Tb	Mb	Eb	Z	La	Ib	Ba	Na
Va	Pa	Db	Nb	Db.												

Now we may turn to Wheel Length 19 -- to the next phase of our solution. Again, let us write the cryptogram horizontally, this time with a "period" of 19, to produce 19 columns; but, in writing the cryptogram we shall keep the class-identifying letter, "a" or "b", with the basic cryptogram letter as shown above.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Na	Ga	Ab	Pb	Yb	Za	Aa	Ta	P	Xb	Hb	Cb	I	Ra	Fb	Sa	Pa	Ba	Ka
Mb	Fb	Jb	Ra	Ma	Ha	J	Ob	Fb	Cb	N	Ja	Eb	Va	Va	Oa	Qa	Db	Mb
Wb	Ea	Ta	Qa	P	Vb	Qb	Tb	B	Qa	Ib	Ma	La	Ga	Oa	Mb	Jb	Hb	Da
Aa	Ua	G	Vb	Ib	Ab	X	Va	Nb	Ha	Ka	Wa	Ha	Ob	Bb	Eb	Sa	Va	Ba
I	Qb	Ib	Eb	N	Ia	Xb	Aa	Ta	Ca	Ha	Hb	Rb	Db	Ra	La	Ga	V	Mb
Xb	Xb	J	Na	Mb	Ga	Ua	Aa	Ba	Db	Vb	Ib	Ha	Ba	Ra	D	Mb	Bb	Nb
D	Ra	Mb	Fa	Aa	Wa	Xa	Vb	Ib	Zb	Va	Oa	Ca	F	Ib	Mb	Lb	X	Sa
Qb	Oa	Pa	Qa	Ua	Xb	Db	Kb	Wa	Va	Wa	I	Rb	Rb	Rb	A	Ca	Lb	Oa
Wa	Aa	Ra	Pb	Xb	Bb	Aa	Ta	Ya	B	Db	Tb	Zb	J	Fa	Ab	Ta	Ra	Xa
Va	Db	Zb	Kb	Ia	Ma	Oa	N	Nb	Xb	Yb	P	Ua	Rb	Za	Wa	Ga	La	Rb
Cb	Sb	Ba	Ra	Ma	L	Wb	Ib	Tb	J	Fa	Rb	Oa	Ka	Aa	Xa	Db	Kb	Qb
Aa	Sa	Da	H	Xb	Ub	Tb	W	Ba	Wb	Ja	Na	Qa	Aa	Yb	Ab	Fb	Ba	Ha
Qa	P	Db	Pb	Sb	F	Ga	Sb	Ha	Qa	Ha	Aa	Ob	Ib	Db	Na	Ja	Fa	G
Zb	Db	Tb	Y	Ua	Db	Aa	Ja	Fa	Aa	Rb	Lb	Zb	Pa	Wa	La	H	Nb	Ib
Qb	I	Ha	Ib	Oa	Qa	Ja	Na	Fb	Cb	Mb	Ga	Qa	La	D	Jb	Cb	Eb	O
Oa	Pb	Ya	Qa	Ra	Ua	Pb	Rb	Lb	Va	Va	Qa	K	Yb	Db	Hb	J	Na	Sb
Ea	Qa	Fa	Ya	Xb	Db	Lb	Ea	Va	Ka	J	Mb	Qb	Ob	E	Ba	Cb	Oa	Ja
Ga	Ma	Ib	Tb	Yb	Ia	Pa	Ha	P	Nb	Ob	Fb	C	Pa	Nb	Va	Ia	Aa	Ka
Ub	Jb	Rb	Ha	Xa	Ua	M	Mb	Ob	Pb	B	Ga	Nb	Ya	Za	Xa	Aa	Pb	Mb
Xb	Va	Fa	Wa	G	Ib	Cb	Gb	N	Ja	Ib	Va	Xa	Aa	Ma	Eb	Mb	Qb	Wa
Ya	Fa	B	Rb	Hb	Db	A	Va	Eb	Ja	Ea	Ra	Va	Sb	Yb	Vb	Aa	La	Wa
X	Sb	Jb	Lb	P	Ra	Wb	Aa	Aa	Oa	La	Lb	Lb	Hb	Pa	Ya	La	V	Yb
Ib	Lb	U	Ka	Ob	Ba	Za	Ma	Ka	Ub	Yb	Db	Ha	Ha	Ja	I	Db	Db	Zb
T	Aa	Zb	Ta	Ga	Ka	Qa	Hb	Ab	Rb	Ha	La	Qa	F	Yb	Eb	Yb	V	Ta
Mb	Ha	Pa	Ia	Wa	Yb	Ob	Jb	Qa	Ua	Ma	D	Sb	Xb	Lb	S	Ba	Wb	Ka
Na	Ka	Ia	Ub	Lb	Wb	Ka	Ja	Ya	H	Sb	Nb	Mb	N	Ha	Ib	Ca	Ja	Na
La	Mb	Fb	Db	Fa	Ja	Ua	R	Db	Qb	Sb	P	Za	Yb	Ja	Ea	Ua	Na	Wb
Lb	Ub	Ga	Sa	Ma	I	Db	Xb	Yb	D	Ya	Jb	La	Ia	Pa	Va	Xb	Ib	Tb
Sa	Ka	Ba	V	Db	Cb	Db	N	Ma	Yb	Ba	Ca	Pa	Ua	Nb	Xb	Rb	Za	Qa
Va	Z	Bb	Kb	Yb	L	Aa	Jb	Ca	Xa	Ra	Aa	Bb	Xb	Vb	Xa	Fa	Va	D
Mb	Jb	Ub	Y	Ua	Ub	Aa	Oa	Ua	Ea	Qb	Ob	Ub	Aa	Ga	Ja	R	Tb	Qb

Db	S	Da	Eb	Da	Aa	Ma	Ka	Nb	Pb	Vb	La	Ba	Va	D	Pb	Mb	Yb	H
Ta	Ab	Qa	Ha	Ba	Za	Vb	Yb	Nb	Ba	Ma	Va	K	Bb	Yb	Nb	M	Ja	Lb
Ra	Ia	Ta	Wa	Yb	Eb	Mb	Ra	Ca	Aa	Q	Ab	Ib	Rb	O	Ja	Tb	Ma	Ba
Pa	Da	Ib	Vb	Jb	Qa	Ua	Aa	G	Lb	Sb	Vb	V	La	Ub	Oa	Ja	Ma	Wa
Rb	Lb	Mb	Wa	Ja	Da	U	Ub	Kb	Ib	N	Oa	Ab	Ma	Ca	Ha	Pa	Tb	Nb
Sb	Ea	La	La	J	Eb	Ob	Lb	F	Ka	Ib	Oa	Ba	Ia	Ga	Kb	Rb	Tb	Ra
Ba	Ja	U	Sb	Hb	Ub	F	Aa	Yb	Ba	Ba	Aa	Sa	Db	Vb	Jb	Ba	Va	Ya
Q	Db	Qb	Eb	C	Ja	Cb	Aa	Fa	Ea	Ka	Tb	Zb	Mb	Aa	Ha	Ea	I	Db
Db	Sb	H	Pa	Cb	Xa	Ba	Ga	Va	Hb	Lb	Mb	La	Da	Ea	G	Tb	Mb	Eb
Z	La	Ib	Ba	Na	Va	Pa	Db	Nb	Db.									

Each of the above 19 columns represent letters which are enciphered with the same pin-setting of Wheel Length 19. In the case of a four-wheel HAGELIN CRYPTOGRAPH system, such as we have here, the letters within a column have come from eight different cipher alphabets; that is, they represent polyalphabeticity of eight alphabets. This, of course, is exactly the same situation as the previous phase of our solution when we were dealing with the 17 columns of Wheel Length 17.

In the present situation, however, we have most of the letters within a column further sub-divided into two groups, those followed by a small-letter "a" and those followed by a small-letter "b". All the letters followed by an "a" have been enciphered with the same pin-setting of Wheel Length 17; and all the letters followed by a "b" have been enciphered with the same pin-setting of Wheel Length 17. Therefore, within one column (of the 19) all letters followed by an "a" have been enciphered with both the same pin-setting of Wheel Length 17 and Wheel Length 19, causing these letters to result from but four cipher alphabets. The same holds true of the letters within the same column followed by the small-letter "b". Thus, within a column all letters followed by the same small-letter are the result of a poly-alphabeticity of four alphabets, the four alphabets being caused by the pin-settings of the remaining two wheels, Wheel Length 21 and Wheel Length 23.

Our problem now is divide the 19 columns into two classes, which we shall arbitrarily term Class C and Class D, where one class represents one pin-setting of Wheel Length 19 and one class represents the other pin-setting of Wheel Length 19. This should be an easier problem than the previous problem of dividing the columns of Wheel Length 17 into two classes, for in this case we already have most of the letters in the two classes, A and B; and in matching columns we can "in effect"

match 52 letters against 52 letters, for each column is comprised of both a 26-letter alphabet of Class A letters and a 26-letter alphabet of Class B letters. In the comparing of columnar frequency distributions, therefore, we shall simultaneously match from one column a 26-letter alphabet of Class A letters and a 26-letter alphabet of Class B letters with similar alphabets in another column.

The frequency distributions of the 19 columns are as follows:

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
#1	"a"	2	1			1		1					1		2	1	1	1	1	1	1		1	1		1	
	"b"			1	2					1			1	3				2	1	1		1	1	1	2		1
#2	"a"	2			1	2	1	1	1	1	1	2	1	1		1		1	1	1		1	1				
	"b"	1			3		1				2		2	1			1	1		3		1			1		
#3	"a"		2		2		2	1	1	1			1				2	1	1		2					1	
	"b"	1	1		1		1			4	2			2				1	1		1	1					2
#4	"a"	1	1				1		2	1		1	1				1	3	2	1	1			3		1	
	"b"				1	3				1		2	1				3		1	1	1	1	2				
#5	"a"	1	1		1		1	1		1	1			3	1	1			1			3		1	1		
	"b"			1	1				2	1	1		1	1		1				1					3	4	
#6	"a"	1	1		1			1	1	2	2	1		1				2	1			2	1	1	1		2
	"b"	1	1	1	3	2				1												3	1	1	1	1	
#7	"a"	5	1					1			1	1		1		1	2	1				3			1		1
	"b"			2	3								1	1		2	1	1			1		1	2	1		
#8	"a"	6				1		1	1		2	1		1	1	1			1		2		2				
	"b"				1			1	1	1	2	1	1	1		1			1	1	1	1	1		1	1	

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
#9	"a"	1	2	2			2		1			1		1				1			1	1	2	1		2	
	"b"	1			1	1	2			1		1	1		5	1					1					2	
#10	"a"	2	2	1		2			1		2	2				1		2				1	2		1		
	"b"			2	2				1	1			1		1		2	1	1			1		1	2	1	1
#11	"a"		2			1	1		3		1	2	1	2					1				2	1		1	
	"b"				1				1	3			1	1		1		1	1	3			2			2	
#12	"a"	3		1				2			1		2	1	1	3		1	1				2	1			
	"b"	1		1	1		1		1	1	1		2	2	1	1			1		2		1				
#13	"a"		2	1					3				3			1	1	3		1		1	1		1		1
	"b"	1	1			1				1			1	1	1	1		1	2	1		1					3
#14	"a"	3	1		1			1	1	2		1	2	1			2		1			1	2			1	
	"b"		1		2				1	1				1		2			3	1					2	2	
#15	"a"	2		1		1	1	2	1		2			1		1	2		2				1	1			2
	"b"		1		2		1			1			1		2				1			1	2			4	
#16	"a"		1			1			2		2		2		1	2				1			2	1	3	1	
	"b"	2				3			1	1	2	1		2	1		1						1		1		
#17	"a"	2	2	2		1	1	2		1	2		1				2	1		1	1	1					
	"b"		1	2	2		1				1		1	2					2		2				1	1	
#18	"a"	1	2				11				2		2	2	2	1			1				3				1
	"b"		1		2	1			1	1		1	1	1	1		1	1			3			1		1	

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
#19	"a"		2		1				1		1	3			1	1		1	1	1	1			3	1	1	
	"b"				1	1				1			1	3	2			2	1	1	1			1		1	1

Instead of making every possible comparison of the frequency distributions of the 19 columns, $\frac{19(19-1)}{2} = 171$ comparisons, let us take the frequency distributions of only the first ten columns and see if we can divide the letters of these columns into two classes which we shall designate Classes C and D.

In comparing Frequency Distribution #1 with Frequency Distribution #2, we may obtain the "sum of the cross-products" as follows:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
#1 "a":	2	1			1		1					1		2	1	1	1	1	1	1		1	1		1	
#2 "a":	2			1	2	1	1	1	1	1	2	1	1		1		1	1	1		1	1				
	4				2		1					1			1		1	1	1			1				

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
#1 "b":			1	2					1			1	3				2	1	1		1	1	1	2		1
#2 "b":	1			3		1				2		2	1			1	1		3		1			1		
				6								2	3				2		3		1			2		

Sum of the cross-products: 4+2+1+1+1+1+1+1+1+6+2+3+2+3+1+2 = 32.

In using the <u>chi</u> test earlier in this chapter, to match the frequency distributions of the letters in the 17 columns of Wheel Length 17, we obtained a quotient by dividing the "sum of the cross-products" by the "product of the lengths of the distributions being matched".

Where the lengths of the distributions being matched are all approximately the same, the "sum of the cross-products" by themselves may be used as validity indexes for matching distributions. Therefore, in the present case we shall use only the "sum of the cross-products" to reach conclusions as to the validity of the frequency distributions being matched.

Thus, with the <u>chi</u> test being made for each pair of frequency distributions of the first ten columns (of the total 19), results are as follows:

#1 + #2 = 32	#1 + #3 = 29	#1 + #4 = 25
#1 + #5 = 24	#1 + #6 = 24	#1 + #7 = 35
#1 + #8 = 35	#1 + #9 = 15	#1 + #10 = 31
#2 + #3 = 23	#2 + #4 = 23	#2 + #5 = 29
#2 + #6 = 31	#2 + #7 = 35	#2 + #8 = 40
#2 + #9 = 20	#2 + #10 = 35	
#3 + #4 = 25	#3 + #5 = 18	#3 + #6 = 23
#3 + #7 = 13	#3 + #8 = 21	#3 + #9 = 23
#3 + #10 = 18		
#4 + #5 = 12	#4 + #6 = 33	#4 + #7 = 22
#4 + #8 = 24	#4 + #9 = 26	#4 + #10 = 26
#5 + #6 = 32	#5 + #7 = 34	#5 + #8 = 32
#5 + #9 = 24	#5 + #10 = 29	
#6 + #7 = 37	#6 + #8 = 27	#6 + #9 = 22
#6 + #10 = 36		
#7 + #8 = 46	#7 + #9 = 20	#7 + #10 = 41
#8 + #9 = 23	#8 + #10 = 36	
#9 + #10 = 29		

In analyzing the above $\frac{10(10-1)}{2} = 45$ _chi_ test results, to divide the ten distributions into the two Classes, C and D, we must remember that the larger the "sum of the cross-products", the more likely it is that the pairs of distributions are in the same class; and conversely, the lesser the "sum of the cross-products", the less likely it is that the pairs of distributions are in the same class.

The first step, obviously, is to make a distribution of the "sum of the cross-products" results. Such a tabulation shows:

(1) the three lowest results are 12, 13, and 15.

(2) the three largest results are 40, 41, and 46.

(3) the average or median result is 26.

As we must start somewhere, let us assume that the three smallest results indicate an incorrect match, and that the three largest results indicate a correct match. We have then:

Correct match	Incorrect match
#2 + #8 = 40	#4 + #5 = 12
#7 + #10 = 41	#3 + #7 = 13
#7 + #8 = 46	#1 + #9 = 15

From these matches we can see:

(1) #4 and #5 are not in the same class.

(2) #1 and #9 are not in the same class.

(3) #2, #7, #8, and #10 are in the same class.

(4) #3 is not in the same class as #2, #7, #8, and #10.

Purely arbitrarily we can consider distributions #2, #7, #8, and #10 as being in Class C, and distribution #3 as in Class D.

Distributions #4 and #5 are assumed not to be in the same class. Let us match these distributions then against distributions #2, #7, #8, and #10 which are in the now designated Class C.

#4 + #2 = 23	#5 + #2 = 29
#4 + #7 = 22	#5 + #7 = 34
#4 + #8 = 24	#5 + #8 = 32
#4 + #10 = 26	#5 + #10 = 29

It appears that almost surely Distribution #5 is within Class C, while Distribution #4 is in Class D. At this point our classes, therefore, are:

Class C: #2, #5, #7, #8, and #10.

Class D: #3 and #4.

Like distributions #4 and #5, distributions #1 and #9, above, are assumed to be in different classes. Therefore, let us match these distributions against those of Class C.

#1 + #2 = 32	#9 + #2 = 20
#1 + #5 = 24	#9 + #5 = 24
#1 + #7 = 35	#9 + #7 = 20
#1 + #8 = 35	#9 + #8 = 23
#1 + #10 = 31	#9 + #10 = 29

From these results it visually appears certainly likely that Distribution #1 is within Class C and that Distribution #9 is within Class D.

Finally, let us match the last unidentified distribution, Frequency Distribution #6 with the now presumed Classes C and D:

Class C	Class D
#6 + #1 = 24	#6 + #3 = 23
#6 + #2 = 31	#6 + #4 = 33
#6 + #5 = 32	#6 + #9 = 22
#6 + #7 = 37	
#6 + #8 = 27	
#6 + #10 = 36	

In spite of (#6 + #1 = 24) and (#6 + #4 = 33), it appears probable that Distribution #6 belongs in Class C; and all ten columns have now been divided into the two Classes C and D as follows:

Class C: #1, #2, #5, #6, #7, #8, and #10.

Class D: #3, #4, and #9.

To this point, we have demonstrated that the pin-settings of wheels in the HAGELIN CRYPTOGRAPH system can be recovered provided only that sufficient ciphertext is available for analysis; and in the case of a four-wheel HAGELIN system, 770 letters of ciphertext (in a single message) is enough to recover the pin-settings of the four wheels. With specific reference to the cryptogram of this chapter, we have to this point --

(1) Recovered the pin-settings of most of the pins of Wheel Length 17.

(2) Recovered the pin-settings of the first ten pins of Wheel Length 19.

The student who has followed closely the procedures so far should have no difficulty in completing the solution of the given cryptogram; and the

only thing he really needs is time!

Before moving on to the next chapter, however, let us "wrap up", so-to-speak, what we have done so far, add a few important points, how to determine the number of "lugs" on a wheel, etc.

Consider the multiple alphabets generated by four wheels with respective lug-settings, for example, of 5, 4, 3, and 1:

Wheel	No. of Lugs	Different Keys Generated
1	5	Ø 5
2	4	Ø 5 + 4 9
3	3	Ø 5 4 9 + 3 8 7 12
4	1	Ø 5 4 9 3 8 7 12 + 1 6 5 10 4 9 8 13

The plus sign (+) represents the additional different keys generated by the additional wheel; but note that the additional wheel must be effective for the additional different keys to be generated. Thus, for example, if all of the pins of the additional wheel are to the left, in a non-effective position, there will be no additional different keys generated.

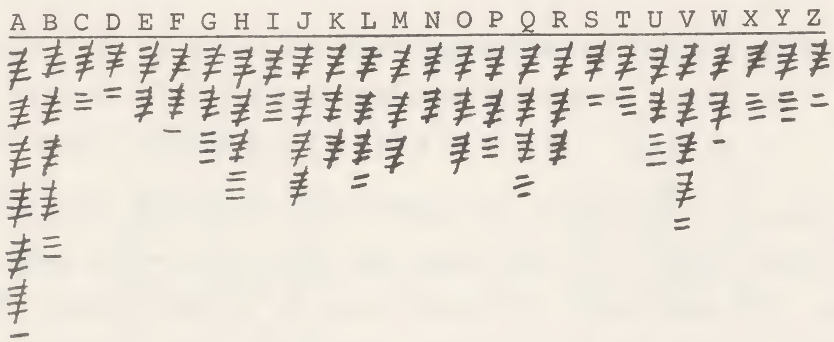
In the first phase of the solution of the cryptogram of the present chapter, the frequency distributions of the 17 columns were divided into two classes, designated A and B. The letters of each column were thus found to be in either Class A or Class B. These classes, in essence, represented the "effectiveness" or "non-effectiveness" of the 17 pins of Wheel Length 17. Turning now to the above, for example, assuming Wheel 4 to be Wheel Length 17, Class A might represent the ciphertext letters generated from the eight alphabets Ø 5 4 9 3 8 7 12. Class A would thus indicate a "non-effectiveness" of Wheel Length 17. Conversely, Class B ciphertext letters would then represent letters generated from the second eight alphabets, these keys being generated from the "effectiveness" of pins on Wheel Length 17.

Several things should be noted especially about these two pairs of eight alphabets, Ø 5 4 9 3 8 7 12 and 1 6 5 10 4 9 8 13. First, one of eight alphabets will always contain the key number Ø. Second, the second of the eight alphabets is the same as the first plus a number representing the number of "lugs" on the wheel.

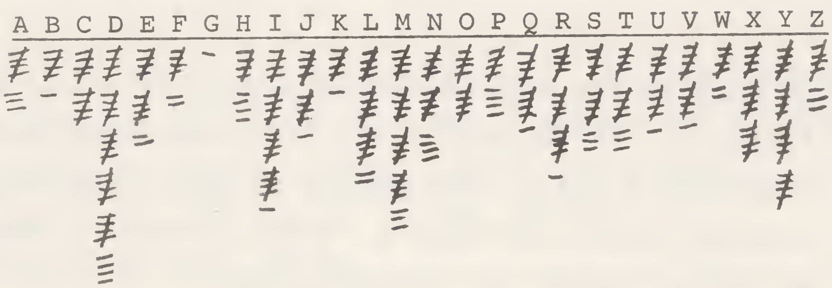
How can we use these facts to our advantage? If one of the eight

always contains the key number Ø, we might expect that the ciphertext letters A and V, representing the plaintext letters Z and E enciphered with a key of Ø, to occur with some degree of frequency within the class representing the eight alphabets generated by a non-effective pin on the wheel. Therefore, let us examine the frequency distributions of all the Class A letters and all the Class B letters from Wheel Length 17.

Class A - (columns 1, 2, 6, 7, 8, 14, 16, 17)



Class B - (columns 3, 4, 5, 10, 11, 12, 15)

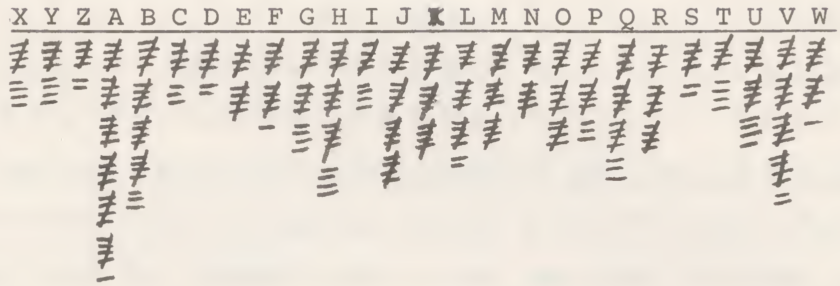


As the Class A distribution, above, contains a large number of A's and V's, it is likely that Class A does represent the eight alphabets containing the key number Ø. The Class B distribution would then represent the second eight alphabets, i.e., the first eight alphabets <u>plus</u> a number representing the number of "lugs" on Wheel Length 17.

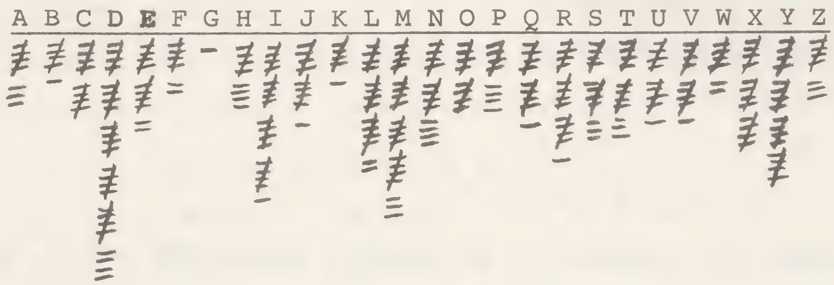
Can we find now the "lug-setting" of Wheel Length 17? Using the fact that Class A + number of "lugs" on Wheel Length 17 = Class B, we can attempt to shift the Class A distribution to the right so that it will equal the Class B distribution, the number of shifts being the number of "lugs" on Wheel Length 17. Visually, it is seen that shifting the Class A distribution to the right three positions will make the two distributions

generally equal, as follows:

Class A - (columns 1, 2, 6, 7, 8, 14, 16, 17)



Class B - (columns 3, 4, 5, 10, 12, 15)



It is likely, therefore, that there are three *lugs* on Wheel Length 17.

The student probably clearly understands now what the Classes A and B represent. But what of the Classes C and D which were involved with Wheel Length 19?

Let us return again to the example generation of multiple alphabets with the four lug-settings, 5, 4, 3, and 1:

Wheel	No. of Lugs	Different keys generated
1	5	Ø 5
2	4	Ø 5 + 4 9
3	3	Ø 5 4 9 + 3 8 7 12
4	1	Ø 5 4 9 3 8 7 12 + 1 6 5 10 4 9 8 13

In this example, if Wheel Length 17 were Wheel 4, Class A = Ø 5 4 9 3 8 7 12 and Class B = 1 6 5 10 4 9 8 13. Assuming Wheel Length 19 = Wheel 3, what different keys are represented by Classes C and D? As above, let us this time show Wheel 3 as the final wheel:

Wheel	No. of Lugs	Different keys generated
1	5	Ø 5
2	4	Ø 5 + 4 9
4	1	Ø 5 4 9 + 1 6 5 10
3	3	Ø 5 4 9 1 6 5 10 + 3 8 7 12 4 9 8 13

Here, Wheel 3 divides the "different keys generated" into the two classes C and D, with C = Ø 5 4 9 1 6 5 10 and D = 3 8 7 12 4 9 8 13, or vice versa. To better show the relationship between the four classes, A, B, C, and D, let us break the different keys generated by each class into two halves, as follows:

A = Ø 5 4 9 + 3 8 7 12

B = 1 6 5 10 + 4 9 8 13

C = Ø 5 4 9 + 1 6 5 10

D = 3 8 7 12 + 4 9 8 13

In the above, for example, if an unknown ciphertext letter is known to be in both Class A and Class C, its key will be one of the four, Ø 5 4 9. Similarly, a ciphertext letter known to be in Class B and Class D must be one of the four keys, 4 9 8 13.

Thus, in the first phase of our solution we succeeded in dividing most of the ciphertext letters into the two Classes A and B. In the second phase we divided the same ciphertext letters into the two Classes C and D with the assistance of knowing that half of the letters in Class C were in Class A with the other half in Class B, and similarly, that half of the letters in Class D were in Class A with the other half in Class B.

By this time, the student should have a good idea of what we have been doing, how a straight mathematical or statistical analysis of an unknown HAGELIN cryptogram operates, etc. We will not continue with the solution of the given cryptogram, since the process is downhill from this point. However, it would be desirable for the student himself to complete the solution, for in the final analysis one can only really learn by doing.

In the problems that follow, all have been enciphered with four effective wheels of the HAGELIN CRYPTOGRAPH.

41. Wheel-Lengths: 23, 21, 19, 17.

E T C K Q   G D K N J   P R W K F   U Q P M G   M A G D F
T A X K I   Y U I J E   F B C N P   K S D Z Z   Q A Q J A
M U Y L F   P M Y F W   B Z V J K   S Y M S K   K P J V T
I P P M A   D U V X J   K J V I E   B E N I Z   E Q J U D
V Y T Y C   J A U W L   R D Y N S   A B B H V   V Z A A D

H U V V F   G P T R P   K V V E W   G E D U R   F F I G J
P J D R I   L E W N L   R M R Z J   S M C L N   C Z Q A O
H E O S M   N D W R V   J Z W V W   G V O U Z   S Y I R C
Z Q J Q P   O U I I Q   A T L I S   Y H K N J   N Y Y L I
G U E R O   Y T J A V   B N Y D W   C C D F L   U O B R F

J P F D R   W F R V U   X X Y A N   O Q L U A   E A D J A
F Z Q Z L   Z N H Y J   P L V T J   V I Y Y X   D Q U X T
U M H R N   E W S J O   O A B U G   F Y S D N   Q D B B X
Z O N H A   R E V Q M   J A V X Z   R V F W K   J Q A S Y
N J D F U   A A J G Y   U A Y U Z   D M E M D   H H S N L

C L V U U   R O Z K O   D F Z C I   F V J E X   U W I Y A
W E V X O   J Y A Q J   R Y M X V   G O O Z Q   F Z V A U
L A Y Q C   C O N S E   H H Z U L   O M G U Q   G P N X W
Y D E R G   C N Q S F   O F I Y P   T D M E E   H R Z J P
P N B K J   C L M F I   P E W L H   K F E O S   F G P V L

N F M E T   S G Y D I   X N D H X   P R J A Q   E A H O X
U D D Z P   V J W K E   D P D D Q   E D R A R   V Z J H X
O U E J E   D F V A A   O O M T W   Z M B P G   K K V A E
R P Z I V   Y Y C Q Y   I N R F A   Q R X U P   V A S K J
D O S N O   M J D M K   L E I E L   M M A E A   E R H T I

A I L A R   R H N O V   P J K F N   D A A U I   K L M U B
P O E A P   U M N Y A   Z J V N P   J F W G Z   L E V Q C
B E H T F   S H F D U   J L O S U   T K G X J   R K G M Y
M N U R I   J A I S J   F T B Y D   Y Q K E J   K P U K K
N Y M M O   F J Z V D   D S U B H   U Q L P K   C R Z A R

M T K C S   J R R Z I   A U I T R   L X K E Y   Z R I S N
W Y Y N R   M K W Q E   Q B T I D   R O Z F D   Z N R J Q
Y U P Q N   R W N Y S   X I H P Z   N E Q W F   N C H P A
R T N R U   A S V F N   G O W V Z   I Q O O I   I K V E I
E D Y V T   Q R T R M   O A N E U   J Z N J M   D F P I A

V Z K A R   G R F D D   Q Z J J N   I E N D F   O Y H E Y
J J H A V   J P O N W   U A C A V   P L O N O   Z U D Q T
G R T R Z   J B Q S E.

42. Wheel-Lengths 23, 21, 19, 17; Both messages enciphered with same initial "wheel settings"; Probable words: "ENEMY", "COMMAND", "MESSAGE", "STOP", "FOR", "TO".

No. 1 - D O D F P   M Y I T R   W D E G G   O V M E Y   K A S C R
V I A X I   M I B T V   Y D X L O   H N M R D   A A T U G
B Z L U J   O M N T X   V B I A U   S Y Z L I   G Z P E V
U D Z J F   B Z O Z G   W Q R C M   N G D A J.

No. 2 - K O B B M   M G N D T   K K X D F   I L I J I   U N Z C R
C S M Y J   Q C B Z K   W Q B S A   T Z F U D   D M S Q F
P B O M P   T L N C Y   I S B W G   O R A K P   G J N Q Z
O D M C N   C R L Z S   C F L H A.

43. Wheel-Lengths: 26, 25, 23, 21; Message begins: "SITUATION REPORT"; Probable words: "KILLED", "WOUNDED", "MISSING".

U U T M H   T S T P F   R Y Y R J   O P S M V   R G D Q Y
M N F A A   A I S B Y   C N P U B   A Y E A P   G B B T Y
T A D E L   R O U C I   X A A L Y   A E V A V   H F S T P.

44. Wheel-Lengths: 25, 23, 21, 19; Message begins: "INTELLIGENCE"; Probable words: "MESSAGE", "INTERROGATION", "ORDER OF BATTLE".

Z M P V X   U X B H U   Y B E T B   Q R O T D   X M M O E
Q B M P W   N C R P B   B S M Y E   E T J G V   J Y Y A J
X T S G Z   V G Q J C   L T S I P   P M T U G   M E L M K
Q R L W X   C Q N M V   C D P D X   F E J C L   H W A B X
X Z P V T   I H Z R Z   H C U X K   F X P V H   G R X O Q
V P N M U   J B S A C   O A S R B   A M D I Y   E L I B N.

45. Wheel-Lengths: 23, 21, 19, 17; Message begins: "WEEKLY SITUATION REPORT"; Probable words: "KILLED", "MISSING": "WOUNDED".

N C J P J   I I C R S   W E X W X   X M T H O   E M G T S
D N P E X   D S A I V   Y I E D F   T J D P U   T J A E A
D X D R A   B P L V D   X Q F A K   B K Y P B   E I D Z T
R D Y D M.

46. Wheel-Lengths: 23, 21, 19, 17; Message begins: "REQUEST"; Probable words: "STOP", "TO", "OF".

Y C S K Y   A Q L S B   S X X V O   F S R Q M   Y N C C P
U C Y Q G   E P G H E   U D C B P   M N C Y X   Y J F Z A
R X K T A   Y W H R E   K H Z L A   D P G M H   U D G P S
B A V Q Q.

47. Probable words: "PRISONER OF WAR", "TO", "ENEMY".

M L J I P   T B P B J   R W B S N   S C O A S   T H S A L
K T U A A   K A S O R   J U L Y K   V T V V F   R C C J J
M I O X L   F C B O F   A M F V K   H X P O X   W K W P T
H L U L S   P R C F D   C D Z D Q   L J O Z S   A J A I M
O I Z V C.

48. Wheel-Lengths: 23, 21, 19, 17; Both messages enciphered with same initial "wheel settings"; Probable words: "ENEMY", "STOP", "ATTACK".

No. 1 - K C F N K   K K L F J   U O K B I   O Q P V V   D C A E N
M B V V W   X I V C G   I N K X X   I S M A Y   T G M L Y
G W G V I   M B L N K   E L I P M   W T I Y H   J I F T Q
Z I D C A   J W B J B   F Y P A L.

No. 2 - Z Y V Y I   I C D S Q   J R K D H   W P W X G   A P G X C
N M Y B A   A S Y L A   E J U C O   A H F Z G   T P Q K O
H J G E R   H A Y A T   X B D P Q.

49. Wheel-Lengths: 23, 21, 19, 17; Probable words: "HEADQUARTERS", "INFORMATION", "ENEMY ATTACK".

Z V O Y E   D V W Z G   L A A A X   E T E P A   U F O X T
R J D Z R   F V H J D   A J N P T   Z X Z C I   Y I X M O
V K R F G   M K O L L   H T C O D   E Q R T J   U D B N J
M V O F Q   F X R R P   J A N I K   J R Q A O   S A R E W
Z F P V R   U X F N I   J B N C F   F I Q G M   W K J W F.

50. Wheel-Lengths: 23, 21, 19, 17; Probable words: "MESSAGE", "STOP", "YOUR".

X A X H M   C C A G V   Z V C H S   W D J I V   Q S I Q B
W Y L P H   B U M O P   W D I L D   A V U Q G   B C G U M
V D A G F   G E A A T   Y V Z M H   V R R I V   D U H I G
W H H A P   G I B C S   F M X E J   G F B O U   M S U H E.

Chapter 6

ANALYSIS OF A FIVE-WHEEL HAGELIN CRYPTOGRAPH

We have now reached the next-to-last stepping stone in our study of the cryptanalysis of the HAGELIN CRYPTOGRAPH. In this chapter we shall consider the cryptanalysis of a five-wheel HAGELIN CRYPTOGRAPH.

Let us consider the solution of the following cryptogram, enciphered with five wheels of lengths 17, 19, 21, 23, and 25. At the same time, to facilitate solution, and to better introduce the student to the principles of *pin-setting* and *lug-setting* reconstruction from recovered generated key, let us be given also the stereotype message beginning (in this case) of "TO COMMANDING GENERAL FIFTH TASK FORCE".

The cryptogram —

```
A U G J S   R E C S A   I R T U T   H P A N M   F I D B U
X Z F K N   L X M A A   N D C O K   T O M J R   K S R D I
F V C S P   Y N S Q E   I V O R C   W E H C P   E F F H W
S Z N W I   Z P I X E.
```

Given ciphertext with a knowledge of plaintext, generated key may be recovered:

Plaintext:	t	o	z	c	o	m	m	a	n	d	i	n	g	z	g	e	n	e	r
Ciphertext:	A	U	G	J	S	R	E	C	S	A	I	R	T	U	T	H	P	A	N
Key:	20	9	6	12	7	4	17	3	6	4	17	5	Ø	20	Ø	12	3	5	5
	a	l	z	f	i	f	t	h	z	t	a	s	k	z	f	o	r	c	e
	M	F	I	D	B	U	X	Z	F	K	N	L	X	M	A	A	N	D	C
	13	17	8	9	10	Ø	17	7	5	4	14	4	8	12	6	15	5	6	7
	z																		
	O																		
	14																		

The recovered generated key looks good! As no individual key is over 20, it appears likely that even with all five wheels effective, the maximum sum of the *lugs* is not over 20.

From this partially recovered generated key let us attempt to determine the *pin-settings* of the five wheels, as well as the number of *lugs* on each wheel.

The first step is to "lay out" the recovered key, similar to the manner described in Chapter 4 as follows:

Recovered key:	20	9	6	12	7	4	17	3	6	4	17	5	Ø	20	Ø	12	3	5	5
Wheel Length (17:																			
(19:																			
(21:																			
(23:																			
(25:																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

13	17	8	9	10	Ø	17	7	5	4	14	4	8	12	6	15	5	6	7	14
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39

It is noted that the individual keys consist of numbers from Ø to 20. The key Ø obviously has arisen from non-effective *pins* on all five wheels; and there is the strong likelihood, conversely, that the key 20 has arisen from effective *pins* on all five wheels. Therefore, in the above "form" we may indicate a non-effective *pin* with a minus sign (-) and an effective *pin* with a plus sign (+) as follows:

	20	9	6	12	7	4	17	3	6	4	17	5	Ø	20	Ø	12	3	5	5	13	17
17:	+												–	+	–						
19:	+												–	+	–						
21:	+												–	+	–						
23:	+												–	+	–						
25:	+												–	+	–						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

	8	9	10	Ø	17	7	5	4	14	4	8	12	6	15	5	6	7	14
17:				–														
19:				–														
21:				–														
23:				–														
25:				–														
	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39

With the "effectiveness" or "non-effectiveness" of *pins* determined for those positions of the recovered key where the key is Ø or 20, the now determined *pins* may be "marked" or indicated throughout the form as follows:

	20	9	6	12	7	4	17	3	6	4	17	5	Ø	20	Ø	12	3	5	5	13	17
17:	+							–					–	+	–			+			
19:	+					–							–	+	–					+	
21:	+			–									–	+	–						
23:	+	–											–	+	–						
25:	+												–	+	–						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

	8	9	10	Ø	17	7	5	4	14	4	8	12	6	15	5	6	7	14
17:				–					–	+	–			+				
19:				–							–	+	–					+
21:				–									–	+	–			
23:				–											–	+	–	
25:				–													–	+
	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39

At this point let us attempt to find a wheel containing an abnormal large number of *lugs*; and thereafter, to determine the *pin-settings* for the wheel.

We begin by writing the recovered key horizontally in a "period" fashion for each of the five wheel lengths. At the same time we note the differences between the largest and smallest key number in each *pin* position as follows:

Wheel Length 17 --

20	9	6	12	7	4	17	3	6	4	17	5	Ø	20	Ø	12	3
5	5	13	17	8	9	10	Ø	17	7	5	4	14	4	8	12	6
15	5	6	7	14												
15	4	7	10	7	5	7	3	11	3	12	1	14	16	8	0	3

Wheel Length 19 --

20	9	6	12	7	4	17	3	6	4	17	5	Ø	20	Ø	12	3	5	5
13	17	8	9	10	Ø	17	7	5	4	14	4	8	12	6	15	5	6	7
14																		
7	8	2	3	3	4	0	4	1	0	3	1	8	8	6	3	2	1	2

Wheel Length 21 --

20	9	6	12	7	4	17	3	6	4	17	5	Ø	20	Ø	12	3	5	5	13	17
8	9	10	Ø	17	7	5	4	14	4	8	12	6	15	5	6	7	14			
12	0	4	12	10	3	12	1	8	0	9	7	6	5	5	6	4	9			

Wheel Length 23 --

20	9	6	12	7	4	17	3	6	4	17	5	Ø	20	Ø	12	3	5	5	13	17	8	9
10	Ø	17	7	5	4	14	4	8	12	6	15	5	6	7	14							
10	9	11	5	2	0	3	1	2	8	11	10	5	14	7	2							

Wheel Length 25 --

20	9	6	12	7	4	17	3	6	4	17	5	Ø	20	Ø	12	3	5	5	13	17	8	9	10	Ø
17	7	5	4	14	4	8	12	6	15	5	6	7	14											
3	2	1	8	11	0	9	9	0	11	12	1	7	6											

It is seen that the wheel length with the *smallest differences* between the largest and smallest key number within each position when the recovered key is written horizontally in wheel length "period" fashion is Wheel Length 19 where the largest difference in any position is eight.

Thus, it appears that Wheel Length 19 contains a relatively large number of *lugs*! And with this knowledge we can tenatively designate each position of Wheel Length 19 as "effective" or "non-effective" as follows:

+	+	-	+	-	-	+	-	-	-	+	-	-	+	-	+	-	-	-
20	9	6	12	7	4	17	3	6	4	17	5	Ø	20	Ø	12	3	5	5
13	17	8	9	10	Ø	17	7	5	4	14	4	8	12	6	15	5	6	7
14																		

Examining the "keys" produced by the "effectiveness" or "non-effectiveness" of Wheel Length 19 indicates that the probable number of *lugs* on Wheel Length 19 is nine! That is, an effective *pin* on Wheel Length 19 has added or contributed "9" to the generated key.

We may now return to the initial recovered key "form" and insert in Wheel Length 19 the value of "9" for an effective *pin* and the value of "0" (which is the same as a minus sign) for a non-effective *pin* as follows:

	20	9	6	12	7	4	17	3	6	4	17	5	Ø	20	Ø	12	3	5	5	13	17
17:	+							-					-	+	-			+			
19:	9	9	0	9	0	0	9	0	0	0	9	0	0	9	0	9	0	0	0	9	9
21:	+			-									-	+	-						
23:	+	-											-	+	-						
25:	+												-	+	-						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

	8	9	10	Ø	17	7	5	4	14	4	8	12	6	15	5	6	7	14
17:				-					-	+	-			+				
19:	0	9	0	0	9	0	0	0	9	0	0	9	0	9	0	0	0	9
21:	+			-									-	+	-			
23:			+	-											-	+	-	
25:				-	+												-	+
	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39

Examining the now partially completed recovered key "form", position 2 with its key of 9 is noted. As the *pin* of Wheel Length 19 in this position has contributed its value of 9 to the total resultant key of 9, the *pins* of the other wheels in this position must be non-effective. Position 2 of Wheel Length 17, thus, must be non-effective; but note position 36 with its key of 5. The *pin* of Wheel Length 17 in position 2 is the same *pin* of Wheel Length 17 in position 36. If this *pin* is non-effective, in position 36 the key of 5 must come completely from Wheel Length 25, as the *pins* of the other wheels in this position are also non-effective. We can say, therefore, that the number of *lugs* on Wheel Length 25 is five!

The recovered key "form", with the *pins* now identified in position 2 (and in position 23 with its total key of 9), and with the value of 5 being inserted for each effective *pin* in Wheel Length 25, now appears as follows:

	20	9	6	12	7	4	17	3	6	4	17	5	Ø	20	Ø	12	3	5	5	13	17
17:	+	-				-		-					-	+	-			+	-		
19:	9	9	0	9	0	0	9	0	0	0	9	0	0	9	0	9	0	0	0	9	9
21:	+	-		-									-	+	-						
23:	+	-											-	+	-						
25:	5	0									5		0	5	0						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

	8	9	10	Ø	17	7	5	4	14	4	8	12	6	15	5	6	7	14
17:		-		-					-	+	-			+	-			
19:	0	9	0	0	9	0	0	0	9	0	0	9	0	9	0	0	0	9
21:	+	-		-									-	+	-			
23:		-	+	-											-	+	-	
25:		0		0	5	0									5		0	5
	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39

As Wheel Length 25 contains five *lugs*, in those positions where the total generated key is less than five, Wheel Length 25 must be non-effective. Thus, in positions 6, 8, 10, 17, 29, and 31, Wheel Length 25 must be non-effective. Position 18 is noted: since Wheel Length 17 is effective, unless this wheel is completely overlapped by Wheel Length 25 (which is known to contain five *lugs*), Wheel Length 25 must be non-effective. These new identifications may be added to the recovered key "form" in all their relative positions; and the "form" to this point appears as follows:

	20	9	6	12	7	4	17	3	6	4	17	5	Ø	20	Ø	12	3	5	5	13	17
17:	+	–				–		–					–	+	–			+	–		
19:	9	9	0	9	0	0	9	0	0	0	9	0	0	9	0	9	0	0	0	9	9
21:	+	–		–									–	+	–						
23:	+	–											–	+	–						
25:	5	0		0		0		0		0	5		0	5	0		0	0			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

	8	9	10	Ø	17	7	5	4	14	4	8	12	6	15	5	6	7	14
17:		–		–					–	+	–			+	–			
19:	0	9	0	0	9	0	0	0	9	0	0	9	0	9	0	0	0	9
21:	+	–		–									–	+	–			
23:		–	+	–											–	+	–	
25:		0		0	5	0		0		0		0		0	5		0	5
	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39

In looking at the now partially completed form, positions 6 and 8 are noted. In position 6, Wheel Lengths 21 and 23 together equal 4; and in position 8, the same two wheels equal 3. Thus, the number of *lugs* on Wheel Lengths 21 and 23 must be one of the following:

	21	23
(a)	3	1
(b)	3	4
(c)	1	3
(d)	4	3

Position 38 is noted. Wheel Lengths 17 and 21 together add up to 7. Therefore, assuming that there is not more than a *two lug* overlap between Wheel Length 17 and 21, Wheel Length 17 "possibilities" may be added to the cases (a) (b) (c) (d), above, as follows:

	21	23	17
(a)	3	1	4/5/6
(b)	3	4	4/5/6
(c)	1	3	6/7
(d)	4	3	3/4/5

Position 31 now provides some valuable information. The number of *lugs* on Wheel Length 17 cannot be over four, as the *pin* of Wheel Length 17 is "effective" in position 31 and the total key in the same position is 4. Thus, case (c), above, where Wheel Length 17 is shown with 6 or 7 *lugs*, is impossible; and with Wheel Length 17 containing not over four *lugs*, the remaining cases can only be as follows:

	21	23	17
(a)	3	1	4
(b)	3	4	4
(d)	4	3	3/4

Can Wheel Length 17 contain three *lugs*? In position 31 it is seen that the *pin* of Wheel Length 17 is "effective" and the total key is 4. If Wheel Length 17 in this position contains three *lugs*, one additional *lug* must be provided by either Wheel Length 21 or Wheel Length 23 to yield the total 4. But in case (d) above, where Wheel Length 17 is shown with three possible *lugs*, neither Wheel Length 21 nor Wheel Length 23 has one *lug*! Therefore, unless there is the sizable overlap of two or three *lugs*, Wheel Length 17 must contain four *lugs*.

Continuing, in positions 1 and 14 it is seen that with "effective" *pins* on all wheels, the total key is 20; and here we are following the premise that the largest evident key has come from the condition of the *pins* of all wheels being "effective". With nine *lugs* on Wheel Length 19 and five *lugs* on Wheel Length 25, if case (a) above is valid, there will be a total overlap "between all wheels" of two *lugs*. If either case (b) or (d), however, is valid, there will be a total overlap "between all wheels" of five *lugs*. Since it is unlikely that there would be an overlap of five *lugs* between five wheels with such small *lug-settings*, only case (a) above can be assumed to be valid. Moreover, if it is assumed that each wheel has a different number of *lugs*, only case (a) provides a different number of *lugs* for each wheel.

The probability is, then, that Wheel Length 17 contains four *lugs*, that Wheel Length 21 contains three *lugs*, and Wheel Length 23 one *lug*. The recovered key "form" may be revised as follows:

	20	9	6	12	7	4	17	3	6	4	17	5	Ø	20	Ø	12	3	5	5	13	17
17:	4	0				0		0					0	4	0			4	0		
19:	9	9	0	9	0	0	9	0	0	0	9	0	0	9	0	9	0	0	0	9	9
21:	3	0		0									0	3	0						
23:	1	0											0	1	0						
25:	5	0		0		0		0		0	5		0	5	0		0	0			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

	8	9	10	Ø	17	7	5	4	14	4	8	12	6	15	5	6	7	14
17:		0		0					0	4	0			4	0			
19:	0	9	0	0	9	0	0	0	9	0	0	9	0	9	0	0	0	9
21:	3	0		0									0	3	0			
23:		0	1	0											0	1	0	
25:		0		0	5	0		0		0		0		0	5		0	5
	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39

From this point, analysis becomes fairly simple. Position 4, for example, indicates that Wheel Length 17 is "effective" (with four *lugs*) in this position; and in order to obtain a generated total key of 12, there must be an "overlap" between Wheel Length 17 and Wheel Length 19 of one *lug*. Position 39 indicates that Wheel Length 17 is "non-effective" in this position, which in turn indicates that position 5 of Wheel Length 17 is likewise "non-effective"; and with Wheel Length 17 "non-effective" in position 5, the generated total key of 7 in the position can only come from the *pins* of Wheel Lengths 21 and 25 being "effective" in the position and there being also an "overlap" of one *lug* between Wheel Length 21 and Wheel Length 25.

Thus, complete recovery of the *pin-settings* and *lug-settings* of all five wheels is practically assured; and the remaining letters of the cryptogram can easily be read. Completing solution is left to the student.

Before proceeding to Chapter 7, the student should attempt to gain proficiency in the art of recovering *pin-settings* and *lug-settings* from partially recovered key by solving several of the problems that follow.

PROBLEMS

51. Wheel-Lengths: 25, 23, 21, 19, 17; Messages enciphered with same initial "wheel settings"; Probable words: "ATTACK", "REQUEST", "ENEMY", "STOP", "FOR", "TO".

No. 1 -
```
I W L H S   B H P B M   C Z X W H   A U B U G   A I V H D
V P R D Y   C E R C N   J T K A R   E L A E Q   L S C K N
M L I I U   R W Q N V   O M I L S   E J T U D   I C M G H
Q C S U R   O E J K Y   O O S Y V   J P Z Z O   H L I N L.
```

No. 2 -
```
Q U N B Q   G M Y M I   Z F O H Y   A U B P T   R O I D Y
E C E M D   T K E T C   Z M K M F   E B M T A   X Q C G E
V J A H O   E X D D R   R A N D S   K R D W P   M S T L W
Q R S P B   H W A D V   W I K I T   I H E Q F   T S V I X
O J V C J   Z I G Q R   X E X L J   P K P R O   K H R A J.
```

No. 3 -
```
O W Y L Q   T M U V T   P H I W H   J T J J Y   A J S O X
J M R H U   W E I P B   S P Z B K   O H M G J   S M O M N
```

R Q F M W   O H N L O   G H W J H   M T G K A   H X N W X
Q I C P C   A I N D V   P L E Y I   W P M D M   S C U G L
R O V Q Q.

52. Wheel-Lengths: 26, 25, 23, 21, 19; Message beginning: "WEEKLY SITUATION REPORT NUMBER ________ STOP".

P M B T A   L U P V Q   U Q Q T C   W M U H W   D P Y M M
Z U M J S   P P Z I K   O F G G Y   M A U Q D   U P P T O
C C Q L V   I C V F Z   L B K P H   T Q M Y N   U H M E A
O G M W C   Z M Q K Y   N N A F U   F R N M F   J M D S R
J H T O H   F Q K S F   W F S R F   H M H V F   C Z E K Z
E T Q A F   B V S I K.

53. Wheel-Lengths: 25, 23, 21, 19, 17; Message begins: "PRISONER OF WAR INTERROGATION REPORT NUMBER _________".

I I P S Z   D Z G L V   V A V Q M   Q Z G O P   I A V L M
V C R H H   D N T D R   R Y Q P E   I J W D F   U R T G T
M Y S G G   E R V D N   E H A N P   P R G Z K   W Z G Z O
A K E P L   Q M O T H   F E R O C   L V D G S   F Y J L B
M T Q X A   S B M Y T   T I P E O   J C F R N   S E N A U
Q I V D V   N O N B X   C J H W Z   C H A Y O   X C I G Y
S Q Z K Y   X J Y K R   G P F V N   D J G B J   V L R L L

54. Wheel-Lengths: 25, 23, 21, 19, 17; Probable words:"ARTILLERY", "ENEMY"; Messages enciphered with same initial "wheel settings."

No. 1 - U M O W K   Y T R Y I   N E Z G V   V A W B F   G S R O M
V B A J D   Z J R D H   J N G E S   L W S U H   D Q T S C
X X I Z Y   E K K I E   P Z.

No. 2 - Y I Z A X   M W A S I   V V R F A   Q H Q V V   S K C B E
D B Y Q I   U D Y P Q   M M G L X   Z Z N X T   N L U Z T
Q X L W H   S K S M.

No. 3 - M V A Q I   R W S Z D   N E R D V   V A R E R   V F Z L D
Q K G D T   E I N A U   S Z X E S   L D I L D   B Q M Q X
L Z P L Q   X A Q W Y   P Z E Q Q   R F L L I   N D C W M
S K B N M   B F M Q S   M T U M D   N N.

55. Wheel-Lengths: 25, 23, 21, 19, 17; Message ends: STOP SIGNED GENERAL WILLIAM DELGADO.

```
W Q B H V   N P R F D   I I A U N   N M W B M   T E J L Q
Y I T O A   P G B Z H   X J T R W   A S F K R   C Y I P X
T Y N C L   Q N C Q L   H F V F I   S P Y R N   P D B U H
G K Y K V   J O B A G   R X Y D U   K W N I G   X Y O G U
```

Chapter 7

ANALYSIS OF THE SIX-WHEEL HAGELIN CRYPTOGRAPH WHERE INDICATORS ARE UNENCIPHERED

We at last have arrived at the problem of solving the six-wheel HAGELIN CRYPTOGRAPH; but in this chapter we shall be given the added "assist" or "advantage" of knowing the *initial wheel-settings* of messages. Thus, from unenciphered indicators we shall know exactly which portions of the keying sequence, running from 1 to 101405850, have been used to encipher given messages.

Consider the solution of the following three cryptograms enciphered with a Model Type C-48 HAGELIN CRYPTOGRAPH:

No. 1 - J Y B T M   H J J I E   A I W I Z   U Q I Y Q   E W A R N
S A U Y Q   D U L J M   V O H B L   H K R M I   L W G Z W
F C V F Q   F O T G K   F O Y G R   P M Z I Z   M J W Z T
W I B C L   F X X E S   M V S S A   H F X X P   B J D H R
A J B Q P.

No. 2 - O E J I F   E J J G J   R M S U E   P T E G B   N R Q X Q
R P A Y U   G Y A F R   Y J E M M   M U A F M   X T I M Q
P W P H W   P K J X J   F L H F D   J R X P T   J E Z G S
R C G W K.

No. 3 - W L O L G   D J J I E   E N R W T   K F S Q D   F W Q G X
D V Z L X   W X F N K   E H F V F   L U L C I   V Y P O M
X A F R J   Y R M V J   N F X E K   T K K O C   W B Y G N
J U H F E   H D B E W   M S O U W   W P C D G   S R D W L
A Z E A A.

The three messages might have been selected from "traffic" perhaps consisting of hundreds of messages, or we might simply have been given these three messages. In any case, the messages have been selected to deliberately present a situation for the purpose of instruction which could arise using the HAGELIN CRYPTOGRAPH. Further — and we need to keep in mind that these messages have been constructed for instructional purposes — let us be given the following known facts:

(1) Each message begins with the word "MESSAGE" followed by one or

more numbers and the word "STOP".

(2) The first two five-letter groups of each cryptogram are *indicator* groups, where —

(a) The first six letters are the unenciphered initial *setting* of the six HAGELIN CRYPTOGRAPH wheels used to encipher the message.

(b) The seventh through tenth letters indicate the number of letters in the message, where A = 1, B = 2, C = 3, etc. Thus, for example, in Message No. 1 the seventh through tenth letters are J J I E. These letters represent 0 0 9 5, meaning that the message consists of 95 letters.

The message *indicators* representing the initial wheel *settings* of the messages, thus, are:

No. 1 - J Y B T M H

No. 2 - O E J I F E

No. 3 - W L O L G D

The first letter of the *indicator* represents the wheel-setting of Wheel Length 26, the second letter represents the wheel-setting of Wheel Length 25, etc.

As the lengths of the six wheels are 26, 25, 23, 21, 19, and 17, there are 26 x 25 x 23 x 21 x 19 x 17 = 101,405,850 possible different "starting points" for the encipherment (or decipherment) of messages. Each "starting point" is represented, thus, by a different initial *setting* of the six wheels; and as the six wheels turn in progression, letters are enciphered (or deciphered) at progressive points along the generated key which is 101,405,850 positions in length.

Our first cryptanalytic task is to convert the above literal *indicators* into <u>successive</u> numerical *indicators*; that is, we want to convert the wheel-setting A A A A A A, for example, into 1, the wheel-setting B B B B B B into 2, C C C C C C into 3... Z Z X U S Q into 101,405,850, etc.

One might visualize, thus, that the 101,405,850 *indicators* represent 101,405,850 successive positions of generated key; and with <u>successive</u> numerical indicators we shall be able to easily see at which points along the 101,405,850 positions of generated key the various messages have been enciphered.

The problem of converting literal *indicators* to successive numerical *indicators* is mathematically not very difficult; and using a "computer" the problem is even less difficult. But the manual conversion process is best described as cumbersome and time consuming!

The process is as follows:

(1) The first step is to replace the letters of the indicators with numbers which represent the positions of the letters on their respective wheels as shown below —

Wheel-Length

26	25	23	21	19	17
A = 1	A = 1	A = 1	A = 1	A = 1	A = 1
B = 2	B = 2	B = 2	B = 2	B = 2	B = 2
C = 3	C = 3	C = 3	C = 3	C = 3	C = 3
D = 4	D = 4	D = 4	D = 4	D = 4	D = 4
E = 5	E = 5	E = 5	E = 5	E = 5	E = 5
F = 6	F = 6	F = 6	F = 6	F = 6	F = 6
G = 7	G = 7	G = 7	G = 7	G = 7	G = 7
H = 8	H = 8	H = 8	H = 8	H = 8	H = 8
I = 9	I = 9	I = 9	I = 9	I = 9	I = 9
J = 10	J = 10	J = 10	J = 10	J = 10	J = 10
K = 11	K = 11	K = 11	K = 11	K = 11	K = 11
L = 12	L = 12	L = 12	L = 12	L = 12	L = 12
M = 13	M = 13	M = 13	M = 13	M = 13	M = 13
N = 14	N = 14	N = 14	N = 14	N = 14	N = 14
O = 15	O = 15	O = 15	O = 15	O = 15	O = 15
P = 16	P = 16	P = 16	P = 16	P = 16	P = 16
Q = 17	Q = 17	Q = 17	Q = 17	Q = 17	Q = 17
R = 18	R = 18	R = 18	R = 18	R = 18	
S = 19	S = 19	S = 19	S = 19	S = 19	
T = 20	T = 20	T = 20	T = 20		
U = 21	U = 21	U = 21	U = 21		
V = 22	V = 22	V = 22			
W = 23	X = 23	X = 23			
X = 24	Y = 24				
Y = 25	Z = 25				
Z = 26					

The three *indicators* thus become:

No. 1 - J Y B T M H = 10 24 2 20 13 8

No. 2 - O E J I F E = 15 5 10 9 6 5

No. 3 - W L O L G D = 23 12 15 12 7 4

(2) We now multiply each number of the obtained numerical indicators

by a given "constant"* for each position of the indicator; and thereafter obtain the sum of the multiplications, as follows:

<u>Indicator No. 1</u>

```
10 x 89705175 =   897051750
24 x 56787276 =  1362894624
 2 x 92587950 =   185175900
20 x 82090450 =  1641809000
13 x 42697200 =   555063600
 8 x 41755350 =   334042800
                 4976037674
```

<u>Indicator No. 2</u>

```
15 x 89705175 =  1345577625
 5 x 56787276 =   283936380
10 x 92587950 =   925879500
 9 x 82090450 =   738814050
 6 x 42697200 =   256183200
 5 x 41755350 =   208776750
                 3759167505
```

<u>Indicator No. 3</u>

```
23 x 89705175 =  2063219025
12 x 56787276 =   681447312
15 x 92587950 =  1388819250
12 x 82090450 =   985085400
 7 x 42697200 =   298880400
 4 x 41755350 =   167021400
                 5584472787
```

(3) The third and final step to obtain the desired <u>successive</u> numerical *indicators* is to divide the sums of the multiplications by 26 x 25 x 23 x 21 x 19 x 17 = 101405850. The remainders of the the divisions will be the <u>successive</u> numerical *indicators*. Thus, the <u>successive</u> numerical *indicators* are found as follows:

<u>No. 1</u> $\frac{4976037674}{101405850}$ = 49 + 7151024. (No. 1 = 7151024)

<u>No. 2</u> $\frac{3759167505}{101405850}$ = 37 + 7151055. (No. 2 = 7151055)

<u>No. 3</u> $\frac{5584472787}{101405850}$ = 55 + 7151037. (No. 3 = 7151037)

---

*These "constants" apply to the Model Type C-48 HAGELIN CRYPTOGRAPH. A machine with wheels of other lengths will have a different set of "constants". Determining these "constants" is a problem within the <u>theory of numbers</u>, and involves solving simultaneous congruences. Chapter V of *Recreations in the Theory of Numbers — The Queen of Mathematics Entertains*, by Albert H. Beiler (Dover) presents a good elementary explanation of the problem.

There is an alternate method to obtain successive numerical *indicators* from unenciphered literal *indicators*. This method eliminates the cumbersome "multiplication step" and is an easier method from a manual viewpoint. The first step is to directly replace the letters of the literal *indicator* with the numbers shown below; and thereafter obtain the sum of the numbers.

Wheel-Length

26	25	23	21	19	17
A=89705175	A=56787276	A=92587950	A=82090450	A=42697200	A=41755350
B=78004500	B=12168702	B=83770050	B=62775050	B=85394400	B=83510700
C=66303825	C=68955978	C=74952150	C=43459650	C=26685750	C=23860200
D=54603150	D=24337404	D=66134250	D=24144250	D=69382950	D=65615550
E=42902475	E=81124680	E=57316350	E=04828850	E=10674300	E=05965050
F=31201800	F=36506106	F=48498450	F=86919300	F=53371500	F=47720400
G=19501125	G=93293382	G=39680550	G=67603900	G=96068700	G=89475750
H=07800450	H=48674808	H=30862650	H=48288500	H=37360050	H=29825250
I=97505625	I=04056234	I=22044750	I=28973100	I=80057250	I=71580600
J=85804950	J=60843510	J=13226850	J=09657700	J=21348600	J=11930100
K=74104275	K=16224936	K=04408950	K=91748150	K=64045800	K=53685450
L=62403600	L=73012212	L=96996900	L=72432750	L=05337150	L=95440800
M=50702925	M=28393638	M=88179000	M=53117350	M=48034350	M=35790300
N=39002250	N=85180914	N=79361100	N=33801950	N=90731550	N=77545650
O=27301575	O=40562340	O=70543200	O=14486550	O=32022900	O=17895150
P=15600900	P=97349616	P=61725300	P=96577000	P=74720100	P=59650500
Q=03900225	Q=52731042	Q=52907400	Q=77261600	Q=16011450	Q=00000000
R=93605400	R=08112468	R=44089500	R=57946200	R=58708650	
S=81904725	S=64899744	S=35271600	S=38630800	S=00000000	
T=70204050	T=20281170	T=26453700	T=19315400		
U=58503375	U=77068446	U=17635800	U=00000000		
V=46802700	V=32449872	V=08817900			
W=35102025	X=89237148	X=00000000			
X=23401350	Y=44618574				
Y=11700675	Z=00000000				
Z=00000000					

Indicator No. 1		Indicator No. 2		Indicator No. 3	
J =	85804950	O =	27301575	W =	35102025
Y =	44618574	E =	81124680	L =	73012212
B =	83770050	J =	13226850	O =	70543200
T =	19315400	I =	28973100	L =	72432750
M =	48034350	F =	53371500	G =	96068700
H =	29825250	E =	05965050	D =	65615550
	311368574		209962755		412774437

The final step to arrive at the successive numerical *indicator* is to subtract from the "sum of the numbers" — but only if the sum is greater than 101405850 — a multiple of 101405850, such that the resulting difference will be less than 101405850. The resulting difference (or sum, if no subtraction is made) is the successive numerical *indicator*.

Thus, one of the following five multiples of 101405850 will be subtracted from a "sum" to result in a difference of less than 101405850:

101405850

202811700

304217550

405623400

507029250

In the case of our three given *indicators*, the successive numerical *indicators* are found as follows:

Indicator No. 1	Indicator No. 2	Indicator No. 3
311368574	209962755	412774437
-304217550	-202811700	-405623400
7151024	7151055	7151037

From the fact that the successive numerical *indicators* are so close together, we can immediately tell that we are fortunate to have what is termed an "overlap" between messages. An "overlap" exists when two messages have been enciphered with the same generated key. Indeed, in the present case we have three messages "overlapping"!

Since we know from the successive numerical *indicators* exactly where each message has been enciphered along the total generated key running from position 1 to position 101405850, we may prepare a worksheet with the messages "in depth"; and knowing that each message begins with the word "MESSAGE" will enable us to "strip off" some generated key as follows:

Position:	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
Key:	13	13	15	1*	Ø*	1*	21	8						17	18	10	15	20	17	10	18
No. 1:	A	I	W	I	Z	U	Q	I	Y	Q	E	W	A	R	N	S	A	U	Y	Q	D
	m	e	s	s	a	g	e	z						z	e	r	o	z	s	t	o
No. 3:														E	N	R	W	T	K	F	S
														m	e	s	s	a	g	e	z

	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68
											4	17	11	13	5	22	24	4						
	U	L	J	M	V	O	H	B	L	H	K	R	M	I	L	W	G	Z	W	F	C	V	F	Q
											t	z	y	e	t	z	r	e						
No. 2:											R	M	S	U	E	P	T	E	G	B	N	R	Q	X
											m	e	s	s	a	g	e	z						
	Q	D	F	W	Q	G	X	D	V	Z	L	X	W	X	F	N	K	E	H	F	V	F	L	U
											s	t	o	p	z	i	n	z						

69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92
F	O	T	G	K	F	O	Y	G	R	P	M	Z	I	Z	M	J	W	Z	T	W	I	B	C
Q	R	P	A	Y	U	G	Y	A	F	R	Y	J	E	M	M	M	U	A	F	M	X	T	I
L	C	I	V	Y	P	O	M	X	A	F	R	J	Y	R	M	V	J	N	F	X	E	K	T

---

*In the generated key a Ø might also be 26; and 1 might be 27.

93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
L	F	X	X	E	S	M	V	S	S	A	H	F	X	X	P	B	J	D	H	R	A	J	B
M	Q	P	W	P	H	W	P	K	J	X	J	F	L	H	F	D	J	R	X	P	T	J	E
K	K	O	C	W	B	Y	G	N	J	U	H	F	E	H	D	B	E	W	M	S	O	U	W

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Q	P.													
Z	G	S	R	C	G	W	K.							
W	P	C	D	G	S	R	D	W	L	A	Z	E	A	A.

It is evident that the messages are correctly aligned "in depth"; and that the portions of generated key so far recovered or "stripped off" are correct. With three messages in depth the problem of recovering key is not particularly difficult. As a last resort, the trial-and-error method of sliding probable words along a message, one letter at a time, until confirmation of the "correctness" of the word is obtained by the text in another message may be tried. With only two messages "in depth" the problem is more difficult, but still generally solvable in time.

In the case of the present three messages, it appears that in Message No. 3 numbers will occur in positions 45 through 54; numbers also will follow the word "MESSAGE" in Message No. 2.

The student may try his own hand at reading the above messages.

For our part, we shall attempt now to recover the *pin and lug settings*, given the recovered key as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
13	13	15	1*	Ø*	1*	21	8	-	-	-	-	Ø*	17	18	10	15	20	17	10	18	10	11	23	1*

26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
21	6	12	17	Ø*	25	4	17	11	13	5	22	24	4	25	10	11	17	10	20	5	17	8	20	13

51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
10	6	12	15	5	22	12	14	17	11	12	13	14	20	6	15	8	19	7	17	10	15	15	9	22

76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
12	15	7	18	9	21	5	22	12	10	19	9	16	12	10	19	10	8	21	15	11	22	6	6	22

101	102	103	104	105	106	107	108
10	23	5	9	21	9	Ø*	Ø*

Let us begin by identifying the wheel or wheels which contain the larger number of *lugs*. We shall take each wheel length in turn, beginning with Wheel Length 17. We write the recovered key horizontally with a "period" of 17 to produce 17 columns —

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
13	13	15	1*	Ø*	1*	21	8	-	-	-	-	Ø*	17	18	10	15
20	17	10	18	10	11	23	1*	21	6	12	17	Ø*	25	4	17	11
13	5	22	24	4	25	10	11	17	10	20	5	17	8	20	13	10
6	12	15	5	22	12	14	17	11	12	13	14	20	6	15	8	19
7	17	10	15	15	9	22	12	15	7	18	9	21	5	22	12	10
19	9	16	12	10	19	10	8	21	15	11	22	6	6	22	10	23
5	9	21	9	Ø*	Ø*											

Column 14 is noted. If Wheel Length 17 contains, for example, seven *lugs*, which we can consider as a "larger number of *lugs*", with a total of 25 in the column, the *pin* of Wheel Length 17 must surely be effective, yet there is also a total of 5 within the same column — which indicates that there cannot be more than five *lugs* on Wheel Length 17! Therefore, Column 14 indicates that Wheel Length 17 in all likelihood does not contain more than five *lugs*. We continue with Wheel Length 19 —

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
13	13	15	1*	Ø*	1*	21	8	-	-	-	-	Ø*	17	18	10	15	20	17
10	18	10	11	23	1*	21	6	12	17	Ø*	25	4	17	11	13	5	22	24
4	25	10	11	17	10	20	5	17	8	20	13	10	6	12	15	5	22	12
14	17	11	12	13	14	20	6	15	8	19	7	17	10	15	15	9	22	12
15	7	18	9	21	5	22	12	10	19	9	16	12	10	19	10	8	21	15
11	22	6	6	22	10	23	5	9	21	9	Ø*	Ø*						

From columns 2 and 12 it appears that Wheel Length 19 might well have seven *lugs*! In any case, Wheel Length 19 cannot have more than seven *lugs*, though it might have six or five.

As it appears likely that Wheel Length 19 does contain seven *lugs*,

let us identify where possible those columns where the *pins* are effective or non-effective. Thus, any column containing a total less than 7 must be non-effective; and it is very likely that any column containing a total of 22 or more will be effective. Note that the total of 22 could arise with a non-effective wheel containing seven *lugs* only if the seven *lugs* contained an "overlap" of two or more *lugs* with one or more other wheels. Indicating effective columns with a plus sign (+) and non-effective columns with a minus sign (-), identifications are as follows:

-	+	-	-	+	-	+	-				+	-	-			-	+	+
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
13	13	15	1*	Ø*	1*	21	8	-	-	-	-	Ø*	17	18	10	15	20	17
10	18	10	11	23	1*	21	6	12	17	Ø*	25	4	17	11	13	5	22	24
4	25	10	11	17	10	20	5	17	8	20	13	10	6	12	15	5	22	12
14	17	11	12	13	14	20	6	15	8	19	7	17	10	15	15	9	22	12
15	7	18	9	21	5	22	12	10	19	9	16	12	10	19	10	8	21	15
11	22	6	6	22	10	23	5	9	21	9	Ø*	Ø*						

It may be noted, also, that with a column identified as to "effectiveness", the ambiguous totals, Ø/26 and 1/27 (Ø* and 1*), will be resolved. Thus, in a non-effective column Ø* will be Ø and 1* will be 1; and in an effective column Ø* will be 26 and 1* will become 27.

The above columns with most of the ambiguous totals resolved will then appear as follows:

-	+	-	-	+	-	+	-				+	-	-			-	+	+
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
13	13	15	1	26	1	21	8	-	-	-	-	Ø	17	18	10	15	20	17
10	18	10	11	23	1	21	6	12	17	Ø*	25	4	17	11	13	5	22	24
4	25	10	11	17	10	20	5	17	8	20	13	10	6	12	15	5	22	12
14	17	11	12	13	14	20	6	15	8	19	7	17	10	15	15	9	22	12
15	7	18	9	21	5	22	12	10	19	9	16	12	10	19	10	8	21	15
11	22	6	6	22	10	23	5	9	21	9	26	Ø						

In similar fashion we can continue with Wheel Length 21, except that this time we can use the "resolved" totals above —

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
13	13	15	1	26	1	21	8	-	-	-	-	Ø	17	18	10	15	20	17	10	18
10	11	23	1	21	6	12	17	Ø*	25	4	17	11	13	5	22	24	4	25	10	11
17	10	20	5	17	8	20	13	10	6	12	15	5	22	12	14	17	11	12	13	14
20	6	15	8	19	7	17	10	15	15	9	22	12	15	7	18	9	21	5	22	12
10	19	9	16	12	10	19	10	8	21	15	11	22	6	6	22	10	23	5	9	21
9	26	Ø																		

Column 19 indicates that Wheel Length 21 has no more than five *lugs*. Let us continue the same procedure with Wheel Length 23 —

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
13	13	15	1	26	1	21	8	-	-	-	-	Ø	17	18	10	15	20	17	10	18	10	11
23	1	21	6	12	17	Ø*	25	4	17	11	13	5	22	24	4	25	10	11	17	10	20	5
17	8	20	13	10	6	12	15	5	22	12	14	17	11	12	13	14	20	6	15	8	19	7
17	10	15	15	9	22	12	15	7	18	9	21	5	22	12	10	19	9	16	12	10	19	10
8	21	15	11	22	6	6	22	10	23	5	9	21	9	26	Ø							

From these columns it appears that Wheel Length 23 might have eight *lugs*! Note especially columns 1 and 8. Just as we did with Wheel Length 19, let us identify where possible the effective and non-effective columns, using the criteria that a column containing a total less than 7 must be non-effective, and a column containing a total of 22 or more will be effective. The results are as follows:

+	−		−	+	−	−	+	−	+	−		−	+	+	−	+		−				−
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
13	13	15	1	26	1	21	8	-	-	-	-	Ø	17	18	10	15	20	17	10	18	10	11
23	1	21	6	12	17	Ø*	25	4	17	11	13	5	22	24	4	25	10	11	17	10	20	5
17	8	20	13	10	6	12	15	5	22	12	14	17	11	12	13	14	20	6	15	8	19	7
17	10	15	15	9	22	12	15	7	18	9	21	5	22	12	10	19	9	16	12	10	19	10
8	21	15	11	22	6	6	22	10	23	5	9	21	9	26	Ø							

The ambiguous Ø* in column 7 becomes resolved as Ø since the *pin* in column 7 is non-effective. We continue with Wheel Length 25:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
13	13	15	1	26	1	21	8	-	-	-	-	Ø	17	18	10	15	20	17	10	18	10	11	23	1
21	6	12	17	Ø	25	4	17	11	13	5	22	24	4	25	10	11	17	10	20	5	17	8	20	13
10	6	12	15	5	22	12	14	17	11	12	13	14	20	6	15	8	19	7	17	10	15	15	9	22
12	15	7	18	9	21	5	22	12	10	19	9	16	12	10	19	10	8	21	15	11	22	6	6	22
10	23	5	9	21	9	26	Ø																	

From columns 5 and 6 it appears that Wheel Length 25 contains one *lug*!

We continue with the final wheel, Wheel Length 26:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
13	13	15	1	26	1	21	8	-	-	-	-	Ø	17	18	10	15	20	17	10	18	10	11	23	1	21
6	12	17	Ø	25	4	17	11	13	5	22	24	4	25	10	11	17	10	20	5	17	8	10	13	10	6
12	15	5	22	12	14	17	11	12	13	14	20	6	15	8	19	7	17	10	15	15	9	22	12	15	7
18	9	21	5	22	12	10	19	9	16	12	10	19	10	8	21	15	11	22	6	6	22	10	23	5	9
21	9	26	Ø																						

Column 3 indicates that the number of *lugs* of Wheel Length 26 is not over five.

Results of our analysis to this point are:

(1) Wheel Length 17 does not contain more than five *lugs*.

(2) It is likely that Wheel Length 19 contains seven *lugs*; and 14 of 19 *pins* have been identified (as to their effectiveness).

(3) Wheel Length 21 does not contain more than five *lugs*.

(4) Wheel Length 23 probably has eight *lugs;* and 17 of the 23 *pins* have been identified (as to their effectiveness).

(5) Wheel Length 25 has been found to contain one *lug.*

(6) Wheel Length 26 contains not more than five *lugs.*

(7) Ambiguous totals Ø/26 and 1/27 (Ø* and 1*) have been resolved.

Just as we did in Chapters 4 and 5, let us now "lay out" in a distinct "form" the so-far recovered key. At the same time we shall bring the "form" up-to-this-point with:

(1) the so-far recovered *pin-settings* of Wheel Lengths 19 and 23.

(2) the assumption that Wheel Length 19 contains seven *lugs*, Wheel Length 23 eight *lugs*, and Wheel Length 25 one *lug*.

(3) the *pins* of all wheels contributing to a key total of Ø to be appropriately indicated as non-effective.

(4) the *pins* of all wheels contributing to a key total of 1 to be indicated as non-effective, except for the *pin* of Wheel Length 25 which will be indicated as effective.

The "form" thus appears as follows:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Recovered key:	13	13	15	1	26	1	21	8	-	-	-	-	Ø	17	18	10	15	20	17
Wheel Length (17:				Ø		Ø		Ø					Ø						
(19:	Ø	7	Ø	Ø	7	Ø	7	Ø			Ø	7	Ø	Ø			Ø	7	7
(21:			Ø	Ø		Ø			Ø				Ø						
(23:	8	Ø		Ø	8	Ø	Ø	8	Ø	8	Ø		Ø	8	8	Ø	8		Ø
(25:				1	Ø	1		Ø					Ø						
(26:				Ø		Ø							Ø						

	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43
	10	18	10	11	23	1	21	6	12	17	Ø	25	4	17	11	13	5	22	24	4	25	10	11	17
		Ø		Ø		Ø					Ø								Ø		Ø		Ø	
	Ø	7	Ø	Ø	7	Ø	7	Ø			Ø	7	Ø	Ø			Ø	7	7	Ø	7	Ø	Ø	7
					Ø	Ø		Ø			Ø				Ø									
				Ø	8	Ø		Ø	8	Ø	Ø	8	Ø	8	Ø		Ø	8	8	Ø	8		Ø	
						1				1	Ø	1		Ø					Ø					
						Ø					Ø		Ø							Ø				

	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67
	10	20	5	17	8	10	13	10	6	12	15	5	22	12	14	17	11	12	13	14	20	6	15	8
				Ø								Ø		Ø		Ø					Ø			
	Ø	7	Ø			Ø	7	Ø	Ø			Ø	7	7	Ø	7	Ø	Ø	7	Ø	7	Ø		
		Ø	Ø		Ø			Ø				Ø											Ø	Ø
			Ø	8	Ø		Ø	8	Ø	Ø	8	Ø	8	Ø		Ø	8	8	Ø	8		Ø		
							1				1	Ø	1		Ø					Ø				
								Ø					Ø		Ø							Ø		

19	7	17	10	15	15	9	22	12	15	7	18	9	21	5	22	12	10	19	9	16	12	10	19
				Ø		Ø		Ø					Ø								Ø		Ø
Ø	7	Ø	Ø			Ø	7	7	Ø	7	Ø	Ø	7	Ø	7	Ø			Ø	7	Ø	Ø	
	Ø			Ø				Ø											Ø	Ø		Ø	
	Ø	8	Ø		Ø	8	Ø	Ø	8	Ø	8	Ø		Ø	8	8	Ø	8		Ø			
							1				1	Ø	1		Ø					Ø			
									Ø					Ø		Ø							Ø
68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91

10	8	21	15	11	22	6	6	22	10	23	5	9	21	9	26	Ø
	Ø					Ø								Ø		Ø
	Ø	7	7	Ø	7	Ø	Ø	7	Ø	7	Ø			Ø	7	Ø
	Ø				Ø											Ø
Ø	8	Ø		Ø	8	Ø	Ø	8	Ø	8	Ø		Ø	8	8	Ø
								1				1	Ø	1		Ø
											Ø					Ø
92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08

--------- 100 ------------

From here the "completion" of the "form" and recovery of the *pin and lug settings* appears inevitable. For example, non-effective *pins* are evident in Position 8. With the total 8 already derived from Wheel Length 23, unless there is a complete "overlap" of *lugs* on another wheel (unlikely), other *pins* in the same position will be non-effective. Numerous other non-effective *pins* can be seen in Positions 69, 78, 93, and 106. With the addition of these non-effective *pins* to the "form" as a whole, final solution appears close. It ia left to the student to complete the "form"; he should have no difficulty.

In this chapter the student has found that one of the HAGELIN CRYPTOGRAPH's vulnerable points is the possibility of an "overlap" between two or more messages — enabling the cryptanalyst to recover key from the messages "in depth" and from this key to recover the original *pin and lug settings*.

In the next chapter we shall discuss a means other than by using unenciphered indicators to put messages "in depth"; and we shall discuss a more general mathematical approach to solving the HAGELIN CRYPTOGRAPH.

PROBLEMS

56. Probable words: "ENEMY", "REQUEST", "SITUATION", "ARTILLERY".

No. 1 - E H U M B F J J I J U M G L J R A K Y H P K X Y R
H X C V J K N T M G T W G L W E S S V D H C M N I
M S T B S V X B H S I H X B X D G L V D K F Q W J
Y J J H G T L N Q I V F W W Y E F Q G S B V Q L U.

No. 2 - L H G F Q   A J J G E   U H I L H   A O I Z Q   T Z J M B
X S Y V Y   B O I L S   L A A O K   B C V S Y   W E Y T E
P U I Y F   M H D T E   S R D E G   L H L O Y   L Q L V D
O R I S I   G L Q Q F.

No. 3 - O K J I S   C J J E E   N L K Y K   Z L M M K   F Y R P C
R P M B C   X I X S D   O J R R W   Y D Q Y L   Y X D N V
R N J R U   B L K V C   C B G I Q.

No. 4 - B F U O F   L J J H J   M M V L G   Z S K M S   U T Q L I
I C Y O H   N V I I U   Z R D Y U   B C H I U   V L K X D
E R Y H R   Y S G W I   Q R O R R   O R T E W   R J N K Q
O L W Z O   T T Q I Z   W D S I W.

No. 5 - I M E A M   B J J C E   B Q G P O   I A K T T   F H Z E N
T X K U O   B H U H M   H A F E R   S L I R Z.

No. 6 - W B S O H   P J J F E   V F D M H   C V G E Y   Q I I F U
Y K X V K   F H T Q H   R S C I J   Q Z F I S   J L L Q H
P L V W W   U L T S U   U F V V E   A E T P M   W P S M B.

No. 7 - L L S E G   C J J F J   V S W P W   S E B O K   B R K O P
E M D S W   Q P I Y X   A G X K X   N T K A R   Y C T T M
N H M C S   A T K L E   T S G P L   D P L G P.

No. 8 - M P F U J   N J J E J   N A V X A   C S N H X   V V Y R L
V Y W V K   M D J B H   T F I P Z   I T A T F   Y J A S T
U U W H M   W W L X J.

No. 9 - W R P N H   E J J E J   I C B I M   V B L V J   R Y E T Y
C D P I Z   U V F K M   Q J F J D   T X Z D M   Y U A Q C
U H T D R   B J L R T

No. 10- F D G J F   M J J E E   A T T N S   N E E W M   N V D U Z
X U Y I A   F R N Q X   B T Q N M   Y I S A B   Q B G T Q
H C C K M   R J Q L Y   Q P B L R.

57. The following four messages have the same streotype beginning.

No. 1 - I X C K P C J J F E U S N G E S J I N X H I W M I
U F O C T X R G K Y O F V L T V X A A W C W S D Z
M E R T G K Q D Q J D T A I G S Z L N E Y S G I O

No. 2 - S H M U G M J J E E N A F H F Z A X F D G D C I F
B F V M A Z X J R A C O F G H H R G G P R P D N U
Y A J N R F Y J O Z T W B I O

No. 3 - A O R C H L J J H J X U M F E V M I N V N G A E M
H O G G B C J Y N P X B T X V Q R H C A X L E S P
J Z A K T A G T I N U V P R P D Z N N X W E B S E
V T L O N C I G I X V Y U I K

No. 4 - S F G K L L J J F E J W L D K Q G P H B I G A N E
S J D D G C I E O O P B U J J H T E Z Z K M T O T
B L W N N H R R B A H E T K N N Y N X O O X X R L

Chapter 8

ANALYSIS OF THE SIX-WHEEL HAGELIN CRYPTOGRAPH GIVEN A SPECIAL SITUATION

When employing any cryptographic system it is difficult, if not impossible, for correspondents *never* to make a mistake. Reasons are many: an inexperienced, untrained individual suddenly finds himself performing complicated cryptographic operations; an experienced, well-trained "cryptographic clerk" suddenly has a lapse of memory and a small error is made; or a situation arises, for example, where a message is enciphered and transmitted by one clerk, and shortly thereafter another clerk transmits the same message a second time.

Consider the following two HAGELIN CRYPTOGRAPH messages which have been transmitted within an hour of each other:

```
No. 1 - B G K T D   W Z V N P   M R E V W   W W R M G   T U K R G
        K B U E C   J J I P R   P V T K P   U T T I U   N F G N U
        A F Z W U   J R G A W   F O M B J   B X Q S F   I W V D W
        B S C G V   S E G R K   A J B Y M   E Q H G L   U H P Y B
        W E W X Q   V D W W H   V Q V G U   U W V V N   L O A U A

        D W N H Y   Q V V T V   J Y L S T   X I N V K   F P K T K
        T M L G Z   L D A B W.

No. 2 - B G K T D   W Z V N P   M R E G F   W T X K T   L O H I F
        J V O B F   V V Q V K   X D E E G   R I R N G   W F H R L
        V N Q T Z   V Y R U X   T N U U P   G M A T B   S L G X X
        P D L M W   C Y J J H   O L B K Z   O U R H H   T B W X G
        V U S M F   W N Q R Z   C V M L T   H K U N E   D V Z W J

        W M K V Z   L U X Q N   S N M W U   R T H U H   N C A H P
        A Q L H I   X C U B W.
```

The cryptanalyst quickly notes that the first 13 letters and last two letters of the messages are similar; and that the lengths of the two messages are the same. The conclusion: the internal plaintext of the messages is the same; and the generated key of the HAGELIN CRYPTOGRAPH could well be the same.

From the point where the two messages differ the next 20 letters may be put "in depth" as follows:

Position:	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
Key:	__	__	__	__	__	__	__	__	__	__	__	__	__	__	__	__	__	__	__	__
No. 1:	V	W	W	W	R	M	G	T	U	K	R	G	K	B	U	E	C	J	J	I
No. 2:	G	F	W	T	X	K	T	L	O	H	I	F	J	V	O	B	F	V	V	Q

We would like "to hope" that the *key* of both messages is the same; and that, therefore, the messages are correctly "in depth". At the same time, we can also "hope" that the plaintext of both messages is the same, <u>except</u> that at Position 14 (where the ciphertext differs) either a letter was added or deleted from one of the messages.

If at this point we assume the *key* in Position 14 to be Ø, the resulting plaintext letters will be:

Position:	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
Key:	Ø	__	__	__	__	__	__	__	__	__	__	__	__	__	__	__	__	__	__	__
No. 1:	V	W	W	W	R	M	G	T	U	K	R	G	K	B	U	E	C	J	J	I
	e																			
No. 2:	G	F	W	T	X	K	T	L	O	H	I	F	J	V	O	B	F	V	V	Q
	t																			

From this point with respect to the plaintext of the messages there are two possibilities:

(1) The plaintext of Message No. 1 from Position 14 is the same as that of Message No. 2 from Position 15 on, or

(2) The plaintext of Message No. 2 from Position 14 is the same as that of Message No. 1 from Position 15 on.

Considering the first possibility, plaintext of both messages will be as follows:

Position:	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
key:	Ø	10	10	7	8	1	8	13	8	21	19	7	10	21	8	15	16	9	21	2
No. 1:	V	W	W	W	R	M	G	T	U	K	R	G	K	B	U	E	C	J	J	I
	e	n	n	k	q	o	b	t	n	k	b	a	z	t	n	k	n	z	l	t
No. 2:	G	F	W	T	X	K	T	L	O	H	I	F	J	V	O	B	F	V	V	Q
	t	e	n	n	k	q	o	b	t	n	k	b	a	z	t	n	k	n	z	l

If we consider the second possibility, plaintext of the two messages will be:

Position:	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
key:	Ø	16	7	7	5	20	16	16	25	21	5	3	8	Ø	25	15	16	20	8	21
No. 1:	V	W	W	W	R	M	G	T	U	K	R	G	K	B	U	E	C	J	J	I
	e	t	k	k	n	h	j	w	e	k	n	w	x	y	e	k	n	k	y	m
No. 2:	G	F	W	T	X	K	T	L	O	H	I	F	J	V	O	B	F	V	V	Q
	t	k	k	n	h	j	w	e	k	n	w	x	y	e	k	n	k	y	m	e

It is evident that the so-called plaintext of both possibilities is incorrect. The text obtained from both possibilities has resulted from the initial assumption that the *key* in Position 14 is Ø. The *key* actually might have been any number from Ø to 25; and from each *key* different plaintext would have resulted

We could individually try in succession each *key* and look for meaningful plaintext; but an easier, more mechanical method would be "to run down the alphabet" starting with the incorrect plaintext obtained in the two possibilities above, and to then look for meaningful plaintext on one of the generatrices obtained.

Negative results are obtained by "running down the alphabet" starting with the incorrect plaintext of the first possibility, as follows:

t	e	n	n	k	q	o	b	t	n	k	b	a	z	t	n	k	n	z	l
u	f	o	o	l	r	p	c	u	o	l	c	b	a	u	o	l	o	a	m
v	g	p	p	m	s	q	d	v	p	m	d	c	b	v	p	m	p	b	n
w	h	q	q	n	t	r	e	w	q	n	e	d	c	w	q	n	q	c	o
x	i	r	r	o	u	s	f	x	r	o	f	e	d	x	r	o	r	d	p
y	j	s	s	p	v	t	g	y	s	p	g	f	e	y	s	p	s	e	q
z	k	t	t	q	w	u	h	z	t	q	h	g	f	z	t	q	t	f	r
a	l	u	u	r	x	v	i	a	u	r	i	h	g	a	u	r	u	g	s
b	m	v	v	s	y	w	j	b	v	s	j	i	h	b	v	s	v	h	t
c	n	w	w	t	z	x	k	c	w	t	k	j	i	c	w	t	w	i	u
d	o	x	x	u	a	y	l	d	x	u	l	k	j	d	x	u	x	j	v
e	p	y	y	v	b	z	m	e	y	v	m	l	k	e	y	v	y	k	w
f	q	z	z	w	c	a	n	f	z	w	n	m	l	f	z	w	z	l	x
g	r	a	a	x	d	b	o	g	a	x	o	n	m	g	a	x	a	m	y
h	s	b	b	y	e	c	p	h	b	y	p	o	n	h	b	y	b	n	z
i	t	c	c	z	f	d	q	i	c	z	q	p	o	i	c	z	c	o	a
j	u	d	d	a	g	e	r	j	d	a	r	q	p	j	d	a	d	p	b
k	v	e	e	b	h	f	s	k	e	b	s	r	q	k	e	b	e	q	c
l	w	f	f	c	i	g	t	l	f	c	t	s	r	l	f	c	f	r	d
m	x	g	g	d	j	h	u	m	g	d	u	t	s	m	g	d	g	s	e
n	y	h	h	e	k	i	v	n	h	e	v	u	t	n	h	e	h	t	f
o	z	i	i	f	l	j	w	o	i	f	w	v	u	o	i	f	i	u	g
p	a	j	j	g	m	k	x	p	j	g	x	w	v	p	j	g	j	v	h
q	b	k	k	h	n	l	y	q	k	h	y	x	w	q	k	h	k	w	i
r	c	l	l	i	o	m	z	r	l	i	z	y	x	r	l	i	l	x	j
s	d	m	m	j	p	n	a	s	m	j	a	z	y	s	m	j	m	y	k

Meaningful plaintext is found on none of the generatrices. Let us turn,

therefore, to the incorrect plaintext obtained from the second possibility above. Again, let us "run down the alphabet" and this time we find success! On one of the generatrices we find real plaintext as follows:

```
e t k k n h j w e k n w x y e k n k y m
f u l l o i k x f l o x y z f l o l z n
g v m m p j l y g m p y z a g m p m a o
h w n n q k m z h n q z a b h n q n b p
i x o o r l n a i o r a b c i o r o c q
j y p p s m o b j p s b c d j p s p d r
k z q q t n p c k q t c d e k q t q e s
l a r r u o q d l r u d e f l r u r f t
m b s s v p r e m s v e f g m s v s g u
n c t t w q s f n t w f g h n t w t h v
o d u u x r t g o u x g h i o u x u i w
p e v v y s u h p v y h i j p v y v j x
q f w w z t v i q w z i j k q w z w k y
r g x x a u w j r x a j k l r x a x l z
s h y y b v x k s y b k l m s y b y m a
t i z z c w y l t z c l m n t z c z n b
u j a a d x z m u a d m n o u a d a o c
v k b b e y a n v b e n o p v b e b p d
w l c c f z b o w c f o p q w c f c q e
x m d d g a c p x d g p q r x d g d r f
y n e e h b d q y e h q r s y e h e s g
z o f f i c e r z f i r s t z f i f t h
a p g g j d f s a g j s t u a g j g u i
b q h h k e g t b h k t u v b h k h v j
c r i i l f h u c i l u v w c i l i w k
d s j j m g i v d j m v w x d j m j x l
```

Thus, in the second possibility, above, with the correct plaintext now identified, the recovered key and messages "in depth" appear as follows:

Position:	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
Key:	21	11	2	2	Ø*	15	11	11	20	16	Ø*	24	3	21	20	10	11	15	3	16
No. 1:	V	W	W	W	R	M	G	T	U	K	R	G	K	B	U	E	C	J	J	I
	z	o	f	f	i	c	e	r	z	f	i	r	s	t	z	f	i	f	t	h
No. 2:	G	F	W	T	X	K	T	L	O	H	I	F	J	V	O	B	F	V	V	Q
	o	f	f	i	c	e	r	z	f	i	r	s	t	z	f	i	f	t	h	z

It is now apparent why the two ciphertext messages are not the same. In Message No. 2 the letter "z", as a word-spacer, was omitted in Position 14.

From this point the problem of recovering the key for the remaining letters of the messages is purely a mechanical process; and with sufficient key recovered, the problem of reconstructing the *pin-settings* for the various wheels, and establishing the number of *lugs* on each

wheel is very straightforward following the method described in Chapter 7.

The completion of the present problem is therefore left to the student.

The cryptanalyst must always be alert to detect the situation just covered, a message being enciphered twice with the same wheel-settings. In the case of a message of any length, it would be very difficult to encipher the same message twice and to have the resulting ciphertexts be absolutely similar. There is always the great probability that a letter here and there will be dropped, added, etc., such that for the cryptanalyst such duplicate messages can only be described as "great finds"! Even an experienced "cryptographic clerk" may often be under the mistaken belief that re-enciphering the same text twice with the same wheel-settings is not a blunder, for he thinks erroneously that the ciphertext will be the same.

The motto, then, for the cryptanalyst is to be alert to detect anything unusual, out of the ordinary; and especially, to look for the case of a message being enciphered twice!

PROBLEMS

58. The following two messages have been intercepted within minutes of each other:

No. 1 -	V I J N O	O J A B J	U C A O A	G F H Y B	X O I S M
	P D I P R	L T E J Y	J K P S B	A V W G Y	T K D B Q
	G B M W J	P L O V B	S A A S G	B R A Y J	T Z B V S
	F P N W M	K P Q S A	C D R U O	H I R Z I	I G D H R
	Y I Z I S	C S U T Z	K X N T J	J D M C H	F L C H L
	V J G J Y				
No. 2 -	V I J N O	O J A A E	U C A O A	G F H Y B	X O I S M
	P D I P R	L T E J Y	J K P S B	A V W G Y	T K D B Q
	G B M W J	P L O V B	M R X H E	G I Q R T	U F R J T
	J V S L L	R P J Q S	N C Y O K	K M A N S	D H X S Q
	J V Q P D	W T I P Y	D P G U A	E X R R C	E L D J U

59. Plaintext of the following three messages is believed to be the same. First word is likely to be "RESISTANCE".

No. 1 - R Q X A R C J A J E H E A A M U S Q P H J X P Q Z
B N I Q R Z T O E O S B S U U A U Y R H S T Y G C
T M M X S R R E K L F C B I Z S S N F N H G G G X
E D D Y L J Q I L Q S O R B X J I O C Z O B J E P
W I A V A Q J U J Q G F M I K.

No. 2 - R Q D A R C J A J E A E H T M U L Q P H Q X W J Z
I G P J R G M V X O Z U S U N A U Y Y H Z M Y N V
A F M E L Y K E R E F C U I Z S Z N M G H N Z N Q
E K W F E J X B L Q L O R B E J P H C G H I C E W
P P T V H J T U C Q G F T I R.

No. 3 - S Q D A R C J A J E A E H R O U N O P F Q V W H Z
G I P J R G M V Z M Z W S U N C U A W H X M W P V
C D M E L W K E R G D C W I Z Q Z L O G J N B N S
E M U F E J V B L Q N O R B E J N H A I H K C G U
P N V V J J J U C Q G H T I R.

CHAPTER 9

ANALYSIS OF THE HAGELIN CRYPTOGRAPH
GENERAL SOLUTION

The general solution of the HAGELIN CRYPTOGRAPH has already been described "in principle" in Chapter 5 where the solution of a hypothetical four-wheel Hagelin machine was discussed. If the reader understands the material presented in Chapter 5, he will have no trouble in understanding the rationale behind the general solution.

Thus, given a cryptogram of sufficient length (the more length, the easier being the general solution), just as was done in Chapter 5, the first step is to analyze the text of the cryptogram divided into the "period" of its shortest wheel-length (so that a maximum amount of text per wheel-pin is obtained). In the case of the Model Type C-48 machine (M-209), the shortest wheel-length is 17. Therefore, 17 distributions are initially obtained from the cryptogram, each representing every 17th letter of ciphertext.

The 17 distributions may be considered as divided into two classes, termed Class A and Class B, where one class represents a "pin" of Wheel 17 in a non-effective (inactive) position, and the other a "pin" in an effective (active) position. The object of initial analysis is to divide or separate the 17 distributions into the two classes.

The reader should here understand the "concept" that for any given number of wheels, there will result ciphertext which will be a "combination" of a given number of different monoalphabetic substitutions. The simplest case, for example, is that of one wheel which results in ciphertext which is a "combination" of two monoalphabetic substitutions, one being the text resulting when the "pin" of the wheel is in a non-effective position (key of Ø) and the other being the text resulting when the "pin" is in an effective position (key = number of "lugs" on wheel). The following table shows the number of different monoalphabetic substitutions which combine to form the result of a given number of wheels:

Number of Wheels	Number of Monoalphabetic Substitutions which Combine
1	2
2	4
3	8
4	16
5	32
6	64

It is seen that the resulting ciphertext of a six-wheel Hagelin system "in effect" is a "combination" of 64 different monoalphabetic substitutions. In the case of the 17 distributions initially obtained from the cryptogram, the letters within a single distribution are the result of the other five wheels and represent a "combination" of 32 monoalphabetic substitutions. That is, text within a single distribution represents a "combination" of 32 different monoalphabetic substitutions. More specifically, Class A represents one set of 32 different monoalphabetic substitutions and Class B represents another set of 32 different monoalphabetic substitutions.

Following the above, the reader should understand the concept of "degree of randomness". Thus, a combination of 32 monoalphabetic substitutions is not purely random, though more random, for example, than if only 16 different monoalphabetic substitutions were combined. In other words, a single monoalphabetic substitution provides ciphertext which is obviously not random, some letters occur more frequently than others, others less frequently, etc. If two different monoalphabetic substitutions are combined, the resulting ciphertext again will not be random, though more random than the single monoalphabetic substitution. If four different monoalphabetic substitutions are combined, again the resulting ciphertext will still not be completely random, and so forth. Therefore, in the case of the 17 distributions, given sufficient text, we should be able to match the distributions into two classes, where one class consists of text resulting from one set of 32 different monoalphabetic substitutions and the other class consists of text resulting from another set of 32 different monoalphabetic substitutions.

In Chapter 5 we were able to match the distributions fairly easily as only four wheels were involved, such that the text within a distribution came from but only eight monoalphabetic substitutions. Since we are now dealing with 32 monoalphabetic substitutions, it is evident that we need more text

to successfully differentiate between the two classes of text. It should also be noted that as the mathematical computations will be much larger than those of Chapter 5, the task of matching distributions in the general solution will probably require use of a computer. In fact, without benefit of a computer, matching distributions in the general solution is a monumental task; not that it cannot be done by hand, however, given sufficient time and manpower.

After successfully dividing the 17 distributions into two classes, in effect we will have found the effective and non-effective "pins" of Wheel 17, though we still will not know which class represents the effective "pins" and which the non-effective "pins".

At this point in solution, using the almost necessary computer we might combine all distributions of one class and combine all distributions of the other class. Then, as was done in Chapter 5, by shifting one of the combined distributions through each of 26 positions, we might attempt to match the two classes of distributions, thus determining the number of "lugs" on Wheel 17.

After initial success with Wheel 17, we might turn to Wheel 19; and following the same procedure, we might attempt to divide the 19 distributions into two classes, i.e., find the "pin-settings" of Wheel 19.

In summary, the general solution follows the general procedure of Chapter 5.

One final point, though we have been up to this point considering a single long cryptogram as forming the text for the general solution, it is possible to combine several shorter cryptograms in order to obtain sufficient text for the general solution. This does <u>not</u> mean, however, that we can simply add, right and left, the texts of different messages. Instead, mathematically, again using the computer, we can attempt to match the 17 distributions of one cryptogram against the 17 distributions of another cryptogram — shifting the distributions of one of the cryptograms through each of 17 "shifts" until the total 17 distributions of one message "match" the total 17 distributions of the other message. At this point Wheel 17 of both cryptograms will be in the same effective position; and for the purpose only of recovering the "pin-settings" of Wheel 17 (separating the 17 distributions into two classes), the two cryptograms may be combined.

We are indebted to Greg Mellen for providing the four problems that follow. All four use the same pin and lug-settings; only the wheel-settings are different for each message. (It is likely that a computer will be required to solve these cryptograms.)

PROBLEMS

```
60.  JAYGZ  DGVHG  XMCRR  HDTSF  SSTMI
     NYCQQ  ECRJQ  HGKTV  JZJBD  TMRLH
     ADUVB  PMXRO  FFZWE  JDYDQ  MWDPN
     JZRQZ  KIRCK  LMJUL  XYXNM  PPEKM
     SIXOQ  MFLSV  PLPVH  TTFWX  ZIDRS

     EJZRU  ODLHP  AIZWN  LVLRB  JIYNC
     KGWYH  BWATY  AYWOW  PNMQS  WLZJE
     XCKDK  IOABG  RMMOP  ZLBDA  RFHAT
     TNHKE  GVSIP  LCCPM  NKNWB  RGBPI
     EEHLT  NAGHB  BMLBE  EQHNS  WFPOR

     JDRMJ  UKYIN  JHSME  YVOTT  QNTHZ
     ESZTN  WPQAD  GGSEH  NMSLH  QVKAQ
     WEJEN  UHIPX  XMOVK  HUJQW  YSPGO
     SLPSK  XUNWB  IMZVC  USYPO  YIHSY
     HSXAK  RGRIH  VROMP  BGJEV  GMPNS

     BDNWV  MSRRC  OGQSI  LUIEU  IIJDX
     MESDE  KLQVR  PJCWW  BQBOJ  CIUGY
     FGOGB  QLSZV  KCDAH  CVOSB  LVQZK
     ULWXW  YTSRP  RWTOZ  BSUGT  HWOVT
     ENWMR  VYMUG  KUTQD  IXJVZ  LWIIL

     CSXCI  FGSNC  CMHWH  WMKIV  QMWAE
     FMMVM  YVQDE  IDYAK  SFQHU  CBUVI
     JJAEO  UNJSY  JJCNZ  IDLSJ  OSVTZ
     XMEHE  ZZOEH  EYLJJ  UGVDN  QXCPP
     HANEE  ZGGAA  TUYVD  HVCDD  ARYKP

     FBENB  XHOPN  KRGLQ  HJVZE  TBSRH
     BZWQG  FAXMK  UCEBJ  PKSMO  UUEYN
     SRZSE  VJFIX  TDQZK  DCQLE  SSTMH
```

FNUWK LHDHS VBVAV QYLMQ KJAGF
MAEBZ EWVAZ OSNMQ FXOIR ZRNGW

HCPCY JTSCB APNPU IXSPW YXOGC
SCCEP QCKVK VXNIF BENTR WOCQQ
HIUWZ MPPWP ZOVWH ZIJLU VRSCG
MPQYC WPPQL ICNNR MOUWW PIKKC
VYZCN BAFAL EBOBU JQQOT UFEPQ

MHIOY XKPCM JEIMI MDPZY JRJPI
QJWLC FEHOP JKGUG HKPKG QTYOM
KYQZX OIKJN KRLTH FRNBY QVAQH
NJHPQ UKYOZ SPOTH NHOIQ HGLXP
EKNDS AAMZR NNAKS HGMXO NNDTG

EVCEY SXACE LPXGC FICYW ZWOVF
EYYWH EVQFL (1035)

61\. DWUVD VRSWY OSKFU HTMQY LSBMD
URBRZ WXEUB IIFTQ WCGRC RXDRN
YBTQB BRKQF LUSBB GVUFZ WFAJL
LTKGL ATFCH PCHOH KFGMO MHHWX
UDYBC XLEMD JDGRI NTVCR FPZLA

TRWGO DNTBN PILHJ HSCTB ENPCQ
ELSLL CWYVO AJPMA HNYAF WPBMB
HFKZA LOPKL VLXUU EJYLA SIBQG
LCNFY PNDGQ FACRR IWOWD NRQXS
ZMOHM NMZHC JQNPE OXJLP PRLNJ

PQRAU DEDQM SUZRU PFSMV CHQES
MTNQN WEKEE GNNYR XQSZA OYRAD
RCLGZ GNKYL JAJDT PUNOF QUGHL
PIKKQ NKWVZ UPMMJ EQSAV AIIPO
DJPLW MCTGC BCTHH HHTVF APRLL

GILYB HVXCU DEVXZ KRTUZ EMEQW
ILHKJ JRASH KENNR QHETN FIJCL
UCAKN LNTWO NFEEC UZWKH YFALI
OEDFC JCGWV XDBGK ZZAWQ YKRJQ
XEXYP WUFSM TETAU CPLHV OCCBR

	WCSAK	GRFBN	OBEZJ	JTNYY	HFZJK
	OCPTS	NVTOR	QEHQW	HKEOM	MMIYL
	EGCBB	HFGBK	POIWH	RJIQO	DOMKB
	AGAPU	AIGDJ	IWJXM	EWJZW	UJOKV
	ECQJE	MXXYK	CCZSB	VTNCA	XRSWG
	PVTEG	RZRXQ	NWYPC	WMCEL	IOQMY
	RENTQ	UVDGT	GNBXH	CSTWD	TTKYQ
	CFSQA	HQJMA	LVRZX	NILPE	XVGIZ
	PEQNJ	HZEEP	WKJEQ	TMIAF	UFIRP
	LVIWY	LOGWW	NYPZH	XEAPU	EBJWL
	XDRJZ	FBCBK	JOMKX	JLCUW	VXNPO
	QVLDM	KWVHL	YRNJP	FBJRW	GLNIH
	OCKYG	HLYTH	GUMOL	AMYUL	XNAUM
	XQYRY	CGSTF	LPMHY	HYDKZ	NLVMZ
	QXPVK	JRVDG	NVKQB	SMEKI	REBBR
	AHZQC	DJNFD	DPLBW	OBQCQ	CNHRO
	VFOLN	MLPZT	MDBOS	MOBIU	XTEVE
	OTIXY	SXAYG	SAJQH	AEIVE	KJSTG
	JHDUV	XNVCJ	YDBYW	EVDYS	QHFIJ
	MDMPA	VQLFF	HVBVX	FQAOR	KYKMV
	CJKRE	LDIVP	MRGTI	MJTGP	VQIYT
	HRSJN	RVVFZ	TQAFZ	FSCNF	NAZJO
	WWQHQ	DARZM	UVDFN	LFRPJ	TRWWU
	NURLI	QABJT	RTNDQ	JMGQJ	SMBGA
	YPSCM	OBSXA	APBMD	KHTLD	USZEQ
	MDZVO	HDLKY	WWSKT	AWYHH	(1145)
62.	ZMGON	MIJOV	RGDVU	GGKKA	VFPVV
	BBMFM	PBPEW	PBRLM	UXZYY	PZIAW
	EIPEZ	KQBPY	KPYVU	NFGZT	ACXEK
	ECIUF	GESHG	PNNZA	FSXMM	WNIOC
	KPDJL	JMRKO	NPJKH	UULLQ	XRQSV
	LVAIJ	JTASA	PGREU	XMFNC	IBSOG
	QLQKC	CFZWJ	PRJOR	VHARN	LCMEN
	GPPYO	BHDXP	AYMAV	JBYYG	OQUBC

HNRDF ZMCAR OAIYB TENLX OLETS
GEHBI EBEXU FFFJL RMRGP KQETZ

BQBNL IJLWA PGPNI PSXUQ UXOTN
ATDAQ REXUN XFZWB YSCSX TERAD
JDLEH RAVCV FKVJU XSLKY HWGZK
GJBBR HNSSS GENVO MZJNI NZKZK
LJHFR HTVUU LVUZI DWBPK FNQDW

PSWLS AGFXQ NYKGD LNOMG NGIRX
AWYBC LLIZB ZHMVA LZNNK HQNEQ
HBSEP VGLLD QCAQF BLDGM KMWYD
PFYXV IUJUW ICGYD VYOHO ZYWBK
PHYRR TIPUA WVLNG BFLZA FUXWA

TDCML OHUPS BJLJR KXXXX (520)

63. BCGSU QTYOG CMAQS LSZEM TKKXW
SVZUM MRDSE THAAP NLYLR SWKHL
JMRSD ITZZW DLYMG AIIJG WZYQX
PNKHQ NGMYO XXJWA JZURN QRBHH
TYTGU MTQVH BVUXK YNZUT MRRTZ

EPQLQ LWUBU OPAKO NRQLG HULWS
VEBEQ VRGPG KUWKT IUGVV OAUKM
MBXTL WUKAM IPGZD CRTUF WWDIM
STTQH TLGUM VQVXG ETETL PXWBX
KACTE NCKEE QMGXL KXBAI EFDWU

SUZLU BUHMM NUXPI ZEKYW FZOYV
VVGUK GLRSP YRHOE MIBJR XPZOR
AKSJI HOGFW ZUXBI GUETS WMBAN
ONXBI CWQYL ITUFY SXWKU EQZFN
RIQSF CLKCW BUENC LODIP OVYPV

UDOXK CITGV ELJQG RHYFQ VZNJC
UITCZ KVCRO WNSIG UTHMU SWBLS
YAVUS LLBNE JBIRV QEQKG DZYCH
ADBSP BZFPO RWZEZ CRVTX LINTB
GBCOY MOCDS WRADH KOWIC RBGJD

SRMHG UAYBV JLNYA RYQWF QICWO
RUOMP VVLAL VNHIF AXXXX (545)

CHAPTER 10

ANALYSIS OF THE HAGELIN CRYPTOGRAPH MODEL TYPE CD-57

A more recent version of the HAGELIN CRYPTOGRAPH is the Model Type CD-57. Louis Kruh, in the July issue of *Cryptologia** describes in some detail the Hagelin Pocket Cryptographer, Type CD-57, as it is termed by its manufacturer. Essentially, the device is a compact unit, 3-1/4" wide, 5-1/8" long, 1-1/2" thick and weighs about 23 ounces. Cryptographically, the CD-57 is in the "family" of HAGELIN CRYPTOGRAPHS, but there are some differences between the CD-57 and, for example, the Model Type C-48 machine (M-209) which has been discussed to this point.

The following *Beaufort Tableau* shows the cryptographic process of the CD-57, where <u>given any two elements, the third element may be found:</u>

BEAUFORT TABLEAU

Key	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0/26	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
1/27	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
2/28	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D
3/29	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E
4/30	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F
5/31	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G
6/32	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H
7/33	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I
8/34	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
9/35	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K
10/36	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
11/37	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M
12/38	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
13/39	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O
14/40	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P
15	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q
16	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R
17	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S
18	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T
19	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U
20	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V
21	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W
22	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X
23	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y
24	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z
25	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

*A quarterly journal devoted to the science of *cryptology*. Address: Albion College, Albion, Michigan 49224.

The reader should compare this *Beaufort Tableau* for the CD-57 with the Hagelin Tableau (also a form of *Beaufort Tableau*) for the Type C-48 Cipher Device (M-209) shown on page 2. Both tableaus are reciprocal; that is, for example, if A + R = a given key, the A may be ciphertext and the R plaintext, or vice versa. But note the differences between the two tableaus:

(1) In the Hagelin Tableau for the Type C-48 Cipher Device (M-209), the possible keys run from Ø to 27, but in the case of the CD-57's *Beaufort Tableau*, the possible keys from from Ø to 40, with the pairs of keys, Ø and 26, 1 and 27, 2 and 28, ... 14 and 40 being the same. Thus, in the CD-57 system a key of 10 and a key of 36 have the same effect insofar as encipherment or decipherment is concerned.

(2) In the Hagelin Tableau for the Type C-48 Cipher Device (M-209), the relationship between letters and the key is fixed; that is, it is invariable that A + R = 18. But in the case of the *Beaufort Tableau* for the CD-57 (and this is not shown on the tableau itself), the realtionships of the letters with the keys shown is true only when the letter A on the "outer alphabet ring" of the CD-57 is exactly at the top of the device. As the "outer alphabet ring" may be turned manually and set at any one of 26 positions for any particular message encipherment/decipherment, the keys shown may be relatively different. Thus, for example, if the letter E on the "outer alphabet ring" is set at the top of the device, rather than the normal letter A, the keys shown in the *Beaufort Tableau* must be increased by 4.

Let us consider now a CD-57 problem. In the July 1977 issue of *Cryptologia*, previously mentioned, Louis Kruh, in addition to describing the Hagelin Pocket Cryptographer, Type CD-57, at the same time offered his readers a "chance to test their cryptanalytic skills" by solving two given messages, both enciphered with the Hagelin Type CD-57 cipher machine. The problem presented by Louis Kruh is the following:

The following two messages were given:

Message Number One

P Z U Y V   N B I Y E   R K G N L   N L E B O   Q Z D W Q
Z V V R D   G Y K N P   R Q X S M   Q T A I G   Y F Z Z V
K X U T N   X K R G I   L Z O Z Q   Q S C O X   E Z N J A

W A T R M B F C W A W K E N Q H H X Z I W Y X G P

O Y X I D N T E W N D N F T P A R L K H T F T N C

C Z C Z W

Message Number Two

O C C A G J Y Q Y M U Z K K N B K E Y K F E E P Q

Z Y W N N G D Z L G Q Y U Z P L T U A M T R F W B

C Z R K D G F T N L Z C O G F K X R W R Y W A Y S

W Z B G M S G A N D E Q Y D A R R X N L Q X F W S

S E R E A G Q T A M Q D T H B Q A M H O F N L F U

W W A S K

In addition, the following information concerning the two messages was provided:

> "The key wheels used have 26, 38, 42, 34, 46 and 25 pins respectively, and less than 50% of each are in active positions. In addition, the key setting of the second half of Message One overlaps with the key setting of the first half of Message Two, and the word artillery is in both of these sections. Other clues may be discerned in the photographs accompanying the text."

The first step, as has been exemplified in most of the problems in previous chapters, is to put the two given messages properly "in depth", then to recover or "strip off" as much keying sequence as possible.

We are given the fact that "the key setting of the second half of Message One overlaps with the key setting of the first half of Message Two." If we take this "fact" to be literally true, since each message contains 130 letters, we can say that the last 65 letters of Message One have been enciphered with the same keying sequence as the first 65 letters of Message Two. Further, we are given the information that the word artillery occurs within the overlap portion of both messages.

Therefore, appropriately overlapping the two messages, we can run the plaintext word artillery through Message Two, simultaneously obtaining resultant text in Message One. When "good" plaintext occurs in Message One, we will know that we have likely found the correct position of the word artillery in Message Two. The following is the result of this tabulation:

Position in Message Two	Message Two	Message One	Resultant plaintext in Message One when word "artillery" occurs in Message Two
1	O	Q	Y B T U U Q D U N
2	C	S	K R F R Q K H G K
3	C	C	A D C N K O T D W
4	A	O	M A Y H O A Q P X
5	G	X	J W S L A X C Q P
6	J	E	F Q W X X J D I R
7	Y	Z	Z U I U J K V K Z
8	Q	N	D G F G K C X S Y
9	Y	J	P D R H C E F R D
10	M	A	M P S Z E M E W A
11	U	W	Y Q K B M L J T A
12	Z	A	Z I M J L Q G T I
13	K	T	R K U I Q N G B H
14	K	R	T S T N N N O A S
15	N	M	B R Y K N V N L Y
16	B	B	A W V K V W Y R A
17	K	F	F T V S U F E T Y
18	E	C	C T D R F L G R Q
19	Y	W	C B C C L N E J P
20	K	A	K A N I N L W I X
21	F	W	J L T K L D V Q M
22	E	K	U R V I D C D F D
23	E	E	A T T A C K S W I
24	P	N	C R L Z K Z J B D
25	Q	Q	A J K H Z Q O W A
26	Z	H	S I S W Q V J T D
27	Y	H	R Q H N V Q G W P
28	W	X	Z F Y S Q N J I A
29	N	Z	O W D N N Q V T Y
30	N	I	F B Y K Q C G R V
31	G	W	K W V N C N E O P
32	D	Y	F T Y Z N L B I K
33	Z	X	C W K K L I V D W
34	L	G	F I V I I C Q P Y
35	G	P	R T T F C X C R O
36	Q	O	C R Q Z X J E H C
37	Y	Y	A O K U J L U V X
38	U	X	X I F G L B I Q O
39	Z	I	R D R I B P D H C
40	P	D	M P T Y P K U V Y
41	L	N	Y R J M K B I R B
42	T	T	A H X H B P E U K
43	U	E	Q V S Y P L H D A
44	A	W	E Q J M L O Q T G
45	M	N	Z H X I O X G Z E
46	T	D	Q V T L X N M X Y
47	R	N	E R W U N T K R U
48	F	F	A U F K T R E N L
49	W	T	D D V Q R L A E Y
50	B	P	M T B O L H R R Y
51	C	A	C Z Z I H Y E R Y
52	Z	R	I X T E Y L E R H

53	R	L	G R P V L L E A V
54	K	K	A N G I L L N O B
55	D	H	W E T I L U B U K
56	G	T	N R T I U I H D F
57	F	F	A R T R I O Q Y H

Success! It is seen that if the word artillery begins in position 23 in Message Two , the resultant plaintext in Message One will be attacks wi, almost surely "good" plaintext. Thus, the overlap with the two messages correctly positioned is as follows:

key-																					
#1 -	Q	S	C	O	X	E	Z	N	J	A	W	A	T	R	M	B	F	C	W	A	W	K
#2 -	O	C	C	A	G	J	Y	Q	Y	M	U	Z	K	K	N	B	K	E	Y	K	F	E
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

key-	4	6	9	7	9	7	17	4	4													
#1 -	E	N	Q	H	H	X	Z	I	W	Y	X	G	P	O	Y	X	I	D	N	T	E	W
	a	t	t	a	c	k	s	w	i													
#2 -	E	P	Q	Z	Y	W	N	N	G	D	Z	L	G	Q	Y	U	Z	P	L	T	U	A
	a	r	t	i	l	l	e	r	y													
	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44

key-																					
#1 -	N	D	N	F	T	P	A	R	L	K	H	T	F	T	N	C	C	Z	C	Z	W
#2 -	M	T	R	F	W	B	C	Z	R	K	D	G	F	T	N	L	Z	C	O	G	F
	45	46	47	48	49	50	51	52	53	45	55	56	57	58	59	60	61	62	63	64	65

By "matching" the word artillery in Message Two against resultant text in Message One, we have recovered a small portion of the keying sequence, the keys between positions 23 and 31. By a "trial-and-error" process we may now attempt to recover additional keying sequence. In essence, we try to guess plaintext in one of the messages, and then confirm the guess by obtaining "good" plaintext in the other message. For example, if we guess that the word enemy comes in front of the word attacks in Message

One, not an unlikely possibility, the letters <u>clude</u> are obtained in Message Two. We are obviously on the right track! Finally, of course, we shall not forget that the word <u>artillery</u> also occurs in Message One. In this manner, some 39 successive keys are quickly recovered as follows:

key-																		6	9	4	8	8
#1 -	Q	S	C	O	X	E	Z	N	J	A	W	A	T	R	M	B	F	C	W	A	W	K
																		e	n	e	m	y
#2 -	O	C	C	A	G	J	Y	Q	Y	M	U	Z	K	K	N	B	K	E	Y	K	F	E
																		c	l	u	d	e
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

key-	4	6	9	7	9	7	17	4	4	17	4	6	6	7	6	8	19	7	4	17	9	4
#1 -	E	N	Q	H	H	X	Z	I	W	Y	X	G	P	O	Y	X	I	D	N	T	E	W
	a	t	t	a	c	k	s	w	i	t	h	a	r	t	i	l	l	e	r	y	f	i
#2 -	E	P	Q	Z	Y	W	N	N	G	D	Z	L	G	Q	Y	U	Z	P	L	T	U	A
	a	r	t	i	l	l	e	r	y	o	f	v	a	r	i	o	u	s	t	y	p	e
	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44

key-	4	7	4	9	9	9	4	9	4	10	15	10									
#1 -	N	D	N	F	T	P	A	R	L	K	H	T	F	T	N	C	C	Z	C	Z	W
	r	e	r	e	q	u	e	s	t	a	i	r									
#2 -	M	T	R	F	W	B	C	Z	R	K	D	G	F	T	N	L	Z	C	O	G	F
	s	o	n	e	n	i	c	k	n	a	m	e									
	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65

A frequency count is made of the 39 recovered keys:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
			11		5	6	2	8	2					1		3		1					

The frequency count brings to light the interesting fact that the number of different keys appears to be limited! Thus, two keys, 4 and 9, account for almost 50% of all keys used; and, indeed, seven keys, 4, 6, 7, 8, 9, 10, and 17, account for almost 95%. From the limited number of different keys appearing, we can make certain deductions:

(1) As no key of Ø appears, which would be the key when all "pins" are non-effective, it appears likely that the "outer alphabet ring" of the CD-57 has been turned so that the letter A does not appear at the top of the device.

(2) Further, as the smallest key, 4, occurs so frequently (11 times), it would appear that 4 might well represent "all wheels non-effective." This being correct, then the letter E on the "outer alphabet ring" of the CD-57 will be at the top of the device, rather than the letter A.

(3) Therefore, reducing all keys by 4, shows that the keying sequence now contains the following adjusted keys: 0, 2, 3, 4, 5, 6, 11, 14, and 15. These are the keys which we shall work with in the second step of our solution, recovering the "pin-settings" of the wheels themselves.

(4)One conclusion which we can reach by examination of these reduced keys is that it appears that the vast majority of pins on the wheels must be in non-effective positions! Thus, it appears that when an adjusted key of 2, 3, 4, 5, or 6 has occurred, it is because only one wheel is active, the others being inactive! Thus, the number of "lugs" on the wheels are likely 2, 3, 4, 5, and 6, with no wheel containing one "lug" (since no adjusted key of 1 occurs).

In the CD-57 system, just as in all the HAGELIN CRYPTOGRAPHS, a key is the result of the summation of the "lugs" (or amount of "kick") of individual active wheels. One important difference, however, between the CD-57 and the previous HAGELIN CRYPTOGRAPHS discussed is that in the CD-57 there are no "overlaps" between wheel "lug-settings." Thus, in the CD-57 system, a resulting key is <u>always</u> the summation of individual wheel lugs, there being no possibility of "overlaps" as were described in Chapter 4. The fact that no "overlaps" are possible in the CD-57 system makes things obviously easier for the cryptanalyst!

The method of recovering "pin-settings" of the wheels is exactly the same as that described in previous chapters. We shall begin by examining the wheel with the fewest number of pins, Wheel 25. (Remember we were given the information that the key wheels used have 26, 38, 42, 34, 46, and 25 pins respectively.) With the 39 recovered keys of the keying sequence put into a "period" of 25 we have the following:

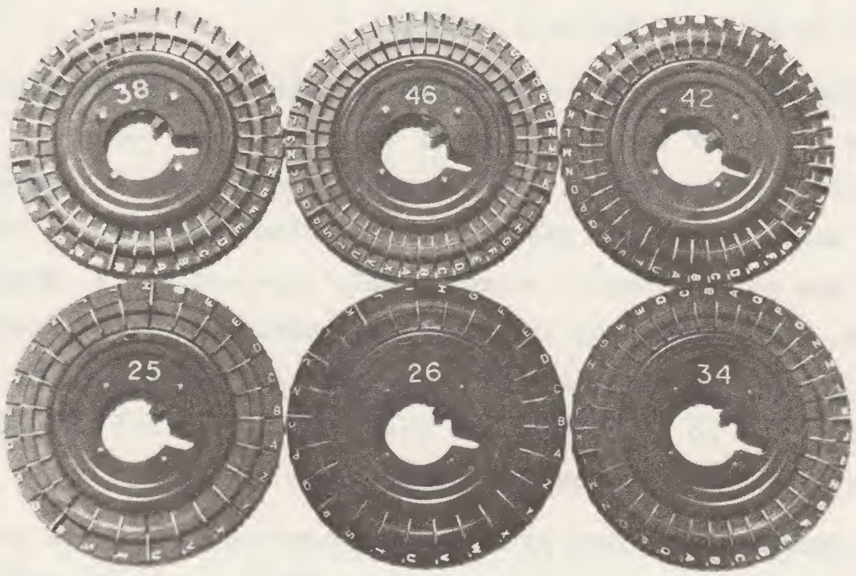
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	5	0	4	4	0	2	5	3	5	3	13	0	0	13	0	2	2	3	2	4	15	3	0	13
5	0	0	3	0	5	5	5	0	5	0	6	11	6											

Since we have reached the conclusion, above, that the number of "lugs" on the wheels likely are 2, 3, 4, 5, and 6 (with no wheel containing one lug),

we might, here, assume or guess that Wheel 25 contains 6 lugs. In other words, if no favorable results are obtained with Wheel 25 containing 6 lugs, for example, we might try Wheel 26 to contain 6 lugs, etc. Therefore, let us assume at this point that Wheel 25 does contain 6 lugs. Then every key less than 6 must be the result of Wheel 25 being non-effective, and the appropriate "pins" may be indicated with a minus (-) sign, as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	5	0	4	4	0	2	5	3	5	3	13	0	0	13	0	2	2	3	2	4	15	3	0	13
5	0	0	3	0	5	5	5	0	5	0	6	11	6											
-	-	-	-	-	-	-	-	-	-	-		-	-		-	-	-	-	-	-		-	-	

It appears that all pins are non-effective, except four, unidentified! Here we take a "short cut"! But who can blame the cryptanalyst for not taking the "path of least resistance"! In the *Cryptologia* article of Louis Kruh (where this problem was offered), there appeared the following picture:



Examining Wheel 25 closely, knowing that pins turned outward toward the rim of the wheel are "effective", we note the following "effective" and "non-effective" pins:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
-	-	-	-	-	-	-	+	-	-	+	-	-	-	-	-	-	+	-	-	+	-	-	-	-

All pins of Wheel 25 are seen to be "non-effective", except four! Will the four "effective" pins now match the four unidentified pins of our

identifications above? Again, success! Wheel 25 matches perfectly the identifications made, and we have the following:

Wheel 25

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	5	0	4	4	0	2	5	3	5	3	13	0	0	13	0	2	2	3	2	4	15	3	0	13
5	0	0	3	0	5	5	5	0	5	0	6	11	6											
-	-	-	-	-	-	-	-	-	-	-	+	-	-	+	-	-	-	-	-	-	+	-	-	+
V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

In a similar manner, the pins of the remaining five wheels may be identified, effective or non-effective; and at the same time, the number of lugs, or the amount of kick, of each wheel may be found.

A portion of the complete cryptographic operation of the CD-57 is shown as follows:

Message One -	Q	S	C	O	X	E	Z	N	J	A	W	A	T	R	M	B	F	C	W	A
	r	r	e	i	n	f	o	r	c	e	m	e	n	t	s	i	f	e	n	e
Message Two -	O	C	C	A	G	J	Y	Q	Y	M	U	Z	K	K	N	B	K	E	Y	K
	t	h	e	w	e	a	p	o	n	s	o	f	w	a	r	i	a	c	l	u
Key -	7	9	6	22	10	9	13	4	11	4	8	4	6	10	4	9	10	6	9	4
Reduced Key -	3	5	2	18	6	5	9	0	7	0	4	0	2	6	0	5	6	2	5	0
Wheel 25 (6) -	-	-	-	+	-	-	+	-	-	-	-	-	-	+	-	-	+	-	-	-
Wheel 46 (5) -	-	+	-	+	-	+	-	-	+	-	-	-	-	-	-	-	-	-	+	-
Wheel 34 (4) -	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Wheel 42 (3) -	+	-	-	+	-	-	+	-	-	-	-	-	-	-	-	+	-	-	-	-
Wheel 38 (2) -	-	-	-	-	+	-	-	-	-	-	+	-	-	-	-	-	-	+	-	-
Wheel 26 (2) -	-	-	+	-	-	-	-	-	+	-	+	-	+	-	-	+	-	-	-	-

Plaintext of Message Two: THE WEAPONS OF WAR IACLUDE ARTILLERY OF
VARIOUS TYPES ONE NICKNAME FOR THESE GUNS
IS LONG RIFLES THE REASON IS THAT THEIR
RANGE CAN EXTEND FOR SEVERAL MILES X.

(One "garbled" letter, incidentally, is noted in the fifth word.)

Concerning solution of the above CD-57 problem, cryptanalysis was assisted by such things as:

(1) The vast majority of "pins" of the wheels were in a non-effective position.

(2) Each wheel contained a very limited number of "lugs".

(3) Knowledge that the overlap portion of both messages contained the word <u>artillery</u>.

(4) Photographs provided the relative position of "pin-settings" on all wheels.

(5) The specific order of the wheels was provided.

Let us now look at another CD-57 problem. This one, a challenge problem, was provided the author by Roger Stuart Brown, MD. This is the problem of Dr. Brown:

```
Cryptogram: M Z A Q Y   J R I S G   A O J C C   T Q P B O   J B S A D
            W O M L X   L J A O U   E U S K B   J P X R E   B U X E C
            Q S M M S   N U G M H   Q S E E M   Q S C Q Z   Z X K D R
            W V Z G F   U Q W K F   Y W R Y X   Z U X G L   Z H C R Q
            G P R L A   Y S P A C   Y E X X X.
```

Given: (1) Message beginning: "TO MY DEAR FRIEND PATRICK ALBERT JOHNSON I SEND TO YOU THE FOLLOWING MESSAGE... "

(2) Having solved one previous cryptogram in the CD-57 system of Dr. Brown, it is likely that the Hagelin Pocket Cryptographer, Type CD-57, used by Dr. Brown to encipher the present message has been used with the letter A of the "outer alphabet ring" at the top of the device, so that the *Beaufort Tableau* on page 93 is directly applicable without any adjustment necessary to the key. Further, it is likely that the following wheels and "lugs" have been used:

Wheel 29 - 1 lug
Wheel 31 - 2 lugs
Wheel 37 - 4 lugs
Wheel 41 - 6 lugs
Wheel 43 - 11 lugs
Wheel 47 - 16 lugs

Let us now solve the problem.

The first step is to recover as much of the keying sequence as possible. Matching the given "message beginning" against the text of the cryptogram, we can easily recover the following keying sequence:

Cryptogram:	M	Z	A	Q	Y	J	R	I	S	G	A	O	J	C	C	T	Q	P	B	O	J
Plaintext:	t	o	m	y	d	e	a	r	f	r	i	e	n	d	p	a	t	r	i	c	k
Key:	5	13	12	14	1	13	17	25	23	23	8	18	22	5	17	19	9	6	9	16	19

B	S	A	D	W	O	M	L	X	L	J	A	O	U	E	U	S	K	B	J	P
a	l	b	e	r	t	j	o	h	n	s	o	n	i	s	e	n	d	t	o	y
1	3	1	7	13	7	21	25	4	24	1	14	1	2	22	24	5	13	20	23	13

X	R	E	B	U	X	E	C	Q	S	M	M	S	N	U	G	M	H	Q	S	E
o	u	t	h	e	f	o	l	l	o	w	i	n	g	m	e	s	s	a	g	e
11	11	23	8	24	2	18	13	1	6	8	20	5	19	6	10	4	25	16	24	8

At this point, let us examine the various "lug totals" (keys) which might arise from the 64 possible "pin-settings" of the six-wheels:

	1	2	4	6	11	16		key		1	2	4	6	11	16		key
1-	0	0	0	0	0	0	=	0	33-	0	0	0	0	0	16	=	16
2-	1	0	0	0	0	0	=	1	34-	1	0	0	0	0	16	=	17
3-	0	2	0	0	0	0	=	2	35-	0	2	0	0	0	16	=	18
4-	0	0	4	0	0	0	=	4	36-	0	0	4	0	0	16	=	20
5-	0	0	0	6	0	0	=	6	37-	0	0	0	6	0	16	=	22
6-	0	0	0	0	11	0	=	11	38-	0	0	0	0	11	16	=	27
7-	1	2	0	0	0	0	=	3	39-	1	2	0	0	0	16	=	19
8-	1	0	4	0	0	0	=	5	40-	1	0	4	0	0	16	=	21
9-	1	0	0	6	0	0	=	7	41-	1	0	0	6	0	16	=	23
10-	1	0	0	0	11	0	=	12	42-	1	0	0	0	11	16	=	28
11-	0	2	4	0	0	0	=	6	43-	0	2	4	0	0	16	=	22
12-	0	2	0	6	0	0	=	8	44-	0	2	0	6	0	16	=	24
13-	0	2	0	0	11	0	=	13	45-	0	2	0	0	11	16	=	29
14-	0	0	4	6	0	0	=	10	46-	0	0	4	6	0	16	=	26
15-	0	0	4	0	11	0	=	15	47-	0	0	4	0	11	16	=	31
16-	0	0	0	6	11	0	=	17	48-	0	0	0	6	11	16	=	33
17-	1	2	4	0	0	0	=	7	49-	1	2	4	0	0	16	=	23
18-	1	2	0	6	0	0	=	9	50-	1	2	0	6	0	16	=	25
19-	1	2	0	0	11	0	=	14	51-	1	2	0	0	11	16	=	30
20-	1	0	4	6	0	0	=	11	52-	1	0	4	6	0	16	=	27
21-	1	0	4	0	11	0	=	16	53-	1	0	4	0	11	16	=	32
22-	1	0	0	6	11	0	=	18	54-	1	0	0	6	11	16	=	34
23-	0	2	4	6	0	0	=	12	55-	0	2	4	6	0	16	=	28
24-	0	2	4	0	11	0	=	17	56-	0	2	4	0	11	16	=	33
25-	0	2	0	6	11	0	=	19	57-	0	2	0	6	11	16	=	35
26-	0	0	4	6	11	0	=	21	58-	0	0	4	6	11	16	=	37
27-	1	2	4	6	0	0	=	13	59-	1	2	4	6	0	16	=	29
28-	1	2	4	0	11	0	=	18	60-	1	2	4	0	11	16	=	34
29-	1	2	0	6	11	0	=	20	61-	1	2	0	6	11	16	=	36
30-	1	0	4	6	11	0	=	22	62-	1	0	4	6	11	16	=	38
31-	0	2	4	6	11	0	=	23	63-	0	2	4	6	11	16	=	39
32-	1	2	4	6	11	0	=	24	64-	1	2	4	6	11	16	=	40

The problem facing the cryptanalyst may be illustrated by turning to the recovered keying sequence, above, and looking apecifically at D + e = 7. Actually, when looking at the *Beaufort Tableau* shown on page 93, it is seen that a key of 7 and a key of 33 are the same. That is, though we have shown that D + e = 7, it might actually have been D + e = 33. Thus, the "pin-setting" giving rise to D + e might be any one of the following four:

	1	2	4	6	11	16		
9-	1	0	0	6	0	0	=	7
17-	1	2	4	0	0	0	=	7
48-	0	0	0	6	11	16	=	33
56-	0	2	4	0	11	16	=	33

It is noted that from D + e = 7/33 not a single pin can be identified as effective or non-effective. But consider other recovered keys. For example, consider in the above keying sequence Q + t = 9. As a key of 9

and a key of 35 are the same, Q + t can only arise from one of the following two "pin-settings":

	1	2	4	6	11	16		
18-	1	2	0	6	0	0	=	9
57-	0	2	0	6	11	16	=	35

Though we are not sure which "pin-setting" has given rise to Q + t, we can say with certainty that —

Wheel 31 with 2 lugs is "effective"

Wheel 37 with 4 lugs is "non-effective"

Wheel 41 with 6 lugs is "effective"

Thus, given the lug-settings 1, 2, 4, 6, 11, and 16, we can prepare a table that will indicate the "effectiveness" of specific lugs when various keys have arisen. The table follows:

	1	2	4	6	11	16
0/26	0	0			0	
1/27		0				
2/28						
3/29		2				
4/30				0		
5/31		0	4	0		
6/32						
7/33						
8/34						
9/35		2	0	6		
10/36				6		
11/37		0				
12/38						
13/39		2				
14/40	1	2			11	
15	0	0	4	0	11	0
16		0		0		
17						
18						
19		2	0			
20						
21		0	4			
22						
23						
24		2		6		
25	1	2	0	6	0	16

Examining the table it is seen that the "effectiveness" of the wheel containing 2 lugs is frequently indicated from the keys. Thus, in our problem the wheel with 2 lugs makes a good "target" for the recovery of

"pin-settings" from the so-far recovered keying sequence. As we know that Wheel 31 contains 2 lugs, we may write the recovered keying sequence in a "period" of 31, and beside each key we may indicate where possible the "effectiveness" of Wheel 31's "pin" in that position:

Position on Wheel 31	1st round of keys	- Pin	2nd round of keys	- Pin	3rd round of keys	- Pin	Composite of Wheel 31's Pin-setting
1	5	0	1	0	8	-	0
2	13	2	14	2			2
3	12	-	1	0			0
4	14	2	2	-			2
5	1	0	22	-			0
6	13	2	24	2			2
7	17	-	5	0			0
8	25	2	13	2			2
9	23	-	20	-			-
10	23	-	23	-			-
11	8	-	13	2			2
12	18	-	11	0			0
13	22	-	11	0			0
14	5	0	23	-			0
15	17	-	8	-			-
16	19	2	24	2			2
17	9	2	2	-			2
18	6	-	18	-			-
19	9	2	13	2			2
20	16	0	1	0			0
21	19	2	6	-			2
22	1	0	8	-			0
23	3	2	20	-			2
24	1	0	5	0			0
25	7	-	19	2			2
26	13	2	6	-			2
27	7	-	10	-			-
28	21	0	4	-			0
29	25	2	25	2			2
30	4	-	16	0			0
31	24	2	24	2			2

An interesting point regarding this recovery of the "pin-settings" of Wheel 31, of which we have to this point recovered all but five "pins", is that in the 2nd round of keys, above, there were numerous confirmations of the "pin-settings" already discovered or found in the 1st round. What this means is that even if we had not known that Wheel 31 contained the 2 lugs, we still could have found it fairly easily because other "periods" would have produced conflicts between the pin-settings found in the 1st and 2nd rounds of keys. In other words, in the present problem, we do

not need to really know the correspondence of wheels to lugs in order to reach a successful solution. Indeed, we do not need to know even the size of the wheels, nor their order for that matter. What is an important fact to know is the number of lugs involved on each wheel. That is, knowing that one wheel contains 1 lug, another 2 lugs, another 4 lugs, another 6 lugs, another 11 lugs, and another 16 lugs are significant facts of great importance for solution! It might be mentioned here that the Operating Instructions of the CD-57 indicate the usual advisability that the sum of the "lugs" on all wheels equal 40. Thus, in the present problem, 1 + 2 + 4 + 6 + 11 + 16 = 40. As the maximum number of "lugs" on one wheel is 16, it can be seen that there is not an unlimited number of "lug" combinations, such that each wheel will have a different number of lugs and that the lugs will total 40. In other words, without overlaps between lug-settings, plus the restrictions on the number of possible lug-combinations, the CD-57 in many respects is less secure than the original Model Type C-48 (M-209) machine.

Returning to the problem, with the "pin-setting" generally recovered on Wheel 31, it is evident that the pin-settings of the remaining wheels are equally vulnerable to analysis — particularly with the already recovered "pin-settings" of Wheel 31 used to assist in identifying other unknown pin-settings. Thus, solution to Dr. Brown's problem is not a real problem from this point; and it is left to the reader-student to continue the soltuion if he desires.

In the following problems, the HAGELIN CRYPTOGRAPH, Model Type CD-57 has been used for encipherments.

PROBLEMS

64. Given: (1) Message stereotype beginning: "TO COMMANDING GENERAL TWENTYFIRST AIRBORNE BRIGADE STOP..."

(2) Wheels and corresponding lugs:
Wheel 29 = 1 lug
Wheel 31 = 2 lugs
Wheel 37 = 4 lugs
Wheel 41 = 6 lugs
Wheel 43 = 11 lugs
Wheel 47 = 16 lugs

```
OTEIA  RYTKT  LVRBG  UFRNE  XLVQC
BSPPB  NBDWV  TXIQG  EQRQM  RZDDZ
```

T Q O K T   T D W M E   W R U X D   V W I K V   K T W I Z
F I M I D   Y C J T P   Z K O D Q   Z S V H Z.

65. Given: (1) Message beginning: "WEEKLY INTELLIGENCE SUMMARY OF FIRST ARMY STOP WEEK OF SIXTEEN JANUARY STOP..."

(2) Lug-settings: 1, 2, 4, 6, 11, 16.

(3) Wheel-lengths: 29, 31, 37, 41, 43, 47 (order unknown).

V U I D Y   T Q C P S   S A U B T   A Q Y X I   G Q G J V
U C A K P   B B N X L   E F I X D   T K S Z A   M G U L N
Z D S K W   J X F A L   T Z E S F   R R V J U   F Z W O E
K O U H L   U I A A Q   Z J J P S   B Q N Z G   E Z Y X Y
V B B D T   J L U F X   V O Z L E   F R V D W   P C J P M
T R B M B   P V P V K   K W Q K X.

66. Given: (1) Message beginning: "IMPORTANT MESSAGE FOR COMMANDING GENERAL STOP..."

(2) Wheels and lugs: Wheel 47 = 1 lug
Wheel 31 = 2 lugs
Wheel 41 = 4 lugs
Wheel 43 = 6 lugs
Wheel 29 = 10 lugs
Wheel 37 = 16 lugs

T R Y U R   V C K Y E   U R T C K   U V A V A   P O R R G
F I H I V   C T A V N   W H J G Y   H N V W Z   T N B I O
Q Y R O F   Q E M U F   H E N I X   Z L T B I   U D S A M
S I C J P   Y G P U V.

67. Given: (1) Four messages "in depth" with lug-settings: 1, 2, 4, 6, 11, 16.

(2) Messages begin: "MESSAGE (number) STOP..."

(3) Wheel lengths: 29, 31, 37, 41, 43, 47 (order unknown).

No. 1 - V Y I U E   E N T G X   A P U E O   W R E H I   N J Y B C
V C I B H   M P W F C   G W O W S   F X B X T   U P G E N
M F S R V   Z V O J A   Z N U T S   R I R L N   Q G J O G
J G F S A   A R Y R A   A F Z Z U   F F A N G   F T X X X.

No. 2 - V Y I U E   E N S S Q   I Q E E O   W R G E V   J M O U N
L M Y G L   N W Y I T   G N M X M   P N Y R U   L R A Z U
L K O T D   U E P I A   U C D G V   K S F T X.

No. 3 - V Y I U E   E N X B Q   B D L E O   W R G O I   K H L F C
M Y C L Y   W D W H A   F Z E Y L   U T Z C N   U X X X X.

No. 4 - V Y I U E   E N G G Z   P G A B D   S N F D I   A X Q N C
C C Y R W   V R R I O   R G Q I V   H O U R T   V R A Z U
B Q S P X   J L D J E   O I T L V   O S E T Z   U X X X X.

68. The following two messages have been intercepted within a few minutes of each other. The enemy has been using lug-settings of 1, 2, 4, 6, 11, 16, and wheel-lengths of 29, 31, 37, 41, 43, 47 (order unknown):

No. 1 - S O G L C   C B H C S   W W P E K   X E E Q E   M C J O J
W N P F G   D Q O Y V   O O Q A A   Y I Q U O   S U Q B Q
T A N W I   T F R V I   Q Z K S C   C I K P X   F C S I U
K E C U Z   V G S I L   A T D Z U   S G T V U   A T H W P
X L I Q K   L P N Q R   F B V Y D   B O N E V   R F W E K
G Q I D V   F R O Y K.

No. 2 - S O G L C   C B H C S   W W P E K   X E E Q E   M C J O J
N Y N G O   G Q X C I   M Q U N J   X K C R M   R R I J A
P Z O N I   W Z T I N   C K Y Q L   F T M D T   E T O A V
T Q O M A   U H N J A   J K L L P   Z T Q D J   T O Q T S
X U N G I   M B Y P S   O F S E C   M D I M Z   I R L K A
M N G C Z   V C D E J   K Q A Q A.

69. Message likely begins: "PRIVATE FOR GENERAL ABERNATHY TAYLOR STOP." The enemy has been using the CD-57 with the following wheels and lugs: Wheel 43 = 1 lug; Wheel 37 = 2 lugs; Wheel 31 = 4 lugs; Wheel 29 = 6 lugs; Wheel 47 = 10 lugs; Wheel 41 = 16 lugs.

S R J B H   S X B Y J   C E E J U   X G X Q C   R O R I Z
K O I K M   Y L S W O   X S A Z G   Q W K Z C   U L M U U
W X Y T W   L X E B Z   N R K B J   N B H C G   R I Z F A
S O K V A   A E E Q D   D N O D K   H H Y D W   W M X C O
R M Z C C.

70. The following message ends with the words: "SIGNED COMMANDING GENERAL FIFTEENTH AIRBORNE STRIKE COMMAND FORCES."

K E Q X Z   P U J U H   O U X Q D   A Q C P Q   F Q E C V
D Z I K F   P P R K K   H M S Y F   X J L T S   V E V N B
K C C G U   Y H P G Z   K N O R T   N Y F C V   Y E V Z O
Z V B B M   Z M Q J Y   J O E J F   O E W C V   E J E T C
Y A N R O   R X X X X.

CHAPTER 11

FINAL REMARKS

In this final chapter we shall attempt to cover several things concerning the solution of the HAGELIN CRYPTOGRAPH which for one reason or the other were not adequately covered in previous chapters. Thus, this chapter may perhaps be described as a *potpourri* of items relating to the HAGELIN CRYPTOGAPH. Also, too, this chapter finally provides the author with an opportunity to present some of his own thoughts or reflections concerning the cryptanalysis of the HAGELIN CRYPTOGRAPH.

First, we should briefly discuss the particular "unusualness" of plaintext which makes up the text of a message enciphered with the Model Type C-48 Hagelin machine (M-209). The "unusualness" of this Hagelin plaintext is caused by using the letter "z" as a space between words. (Enciphering the letter "z" between words causes the plaintext to be printed in normal word-lengths when the message is deciphered.) So non-normal in fact is Hagelin plaintext that the mathematical approach in the general solution can easily be described as extremely effective! Thus, statistical tests used in matching distributions, such as the Chi test, are decidedly more accurate than if the text were simply normal English text without the letter "z" between words.

Based on a distribution of 50,000 letters of English military text in some 9,619 words with the letter "z" being used as a space between words, the average frequencies of 1000 letters are the following:

A - 62	J - 1	S - 51
B - 8	K - 2	T - 77
C - 26	L - 31	U - 22
D - 35	M - 21	V - 13
E - 109	N - 67	W - 13
F - 24	O - 63	X - 4
G - 14	P - 22	Y - 16
H - 28	Q - 3	Z - 162
I - 62	R - 64	

By examining these expected frequencies of letters in Hagelin plain-text, it will be seen that two letters (E and Z) comprise over 25% of the text! And, indeed, the six letters, E, N, O, R, T, and Z, comprise over 50% of the text! Thus, with the abnormal high-frequency of the letter Z especially, one can understand that the statistical tests used in analyzing HAGELIN CRYPTOGRAPH traffic, such as the Chi test, for example, are very successful in matching distributions even when the amount of available text is somewhat limited.

Let us turn now briefly to another important subject in the cryptanalysis of the HAGELIN CRYPTOGRAPH. This is the subject of *enciphered indicators*. In the course of this text we have not seriously touched upon the various cryptanalytic problems involved when *initial wheel-settings of messages* have been enciphered. Thus, in actual practice it is likely that correspondents will have developed or contrived some method to encipher the *initial wheel-settings of messages*.

With respect to these *enciphered indicators*, the cryptanalyst will likely be faced with the following problems:

(1) Attempts can be made to put messages "in depth" or to equate messages by their indicators, even though the indicators are enciphered. In other words, a particular system or method used to encipher the indicators may have a serious "flaw" which will still permit the analyst to benefit from the indicators in some fashion. Thus, just because the indicators have been enciphered does not always mean that the cryptanalyst cannot benefit from them. There are weak "indicator enciphering methods" just as there are weak "cryptographic systems".

(2) After solving a HAGELIN CRYPTOGRAPH message the cryptanalyst of course is always particularly anxious to "recover" the indicator enciphering method so that thereafter he can "read" all the traffic as easily as the correspondents.

The subject of *enciphered indicators* can sometimes be as complex as the subject of solving the HAGELIN CRYPTOGRAPH — and the reader-student is advised that reading one HAGELIN CRYPTOGRAPH message in a particular system does not insure that all messages in the system will be read.

When analyzing and working with *enciphered indicators*, a very important table is the following which shows the relationship between the "wheel-settings" as viewed on the face of the machine and the "effective" pin-

positions internally within the machine that actually affect operations of the machine:

Wheel 26

Letter showing: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Internal pin: P Q R S T U V W X Y Z A B C D E F G H I J K L M N O

Wheel 25

Letter showing: A B C D E F G H I J K L M N O P Q R S T U V X Y Z
Internal pin: O P Q R S T U V X Y Z A B C D E F G H I J K L M N

Wheel 23

Letter showing: A B C D E F G H I J K L M N O P Q R S T U V X
Internal pin: N O P Q R S T U V X A B C D E F G H I J K L M

Wheel 21

Letter showing: A B C D E F G H I J K L M N O P Q R S T U
Internal pin: M N O P Q R S T U A B C D E F G H I J K L

Wheel 19

Letter showing: A B C D E F G H I J K L M N O P Q R S
Internal pin: L M N O P Q R S A B C D E F G H I J K

Wheel 17

Letter showing: A B C D E F G H I J K L M N O P Q
Internal pin: K L M N O P Q A B C D E F G H I J

Let us turn now to the word *faith*! If there is one thing that can be said about almost every cryptographic system, it is that its inventor, its creator, or its backers will have an almost unbelievable amount of *faith* that their system provides the greatest security possible! They will very honestly and naturally believe their system is the best. Moreover, it is extremely difficult, if even possible, to dissuade them from their beliefs. What often happens is that the cryptanalyst finds a "weak spot" in the cryptographic system, and proves the weakness by reading perhaps some messages. The creators of the system will still claim the invincibility of their system and will perhaps "plug the leak" so-to-speak by making a change in their system which may prevent the cryptanalyst from solving the system in the manner in which he original reached a solution. But as you might suspect, a new weakness is either introduced into the system, or is found by the cryptanalyst, and the system is again solved! Consider now the case of the HAGELIN CRYPTOGRAPH.

The original HAGELIN CRYPTOGRAPH consisted of five-wheels. A short while later the Model Type C-48 cipher machine (M-209) came into existence with six keywheels having respectively 26, 25, 23, 21, 19, and 17 pins. Then came the more complicated models, to "plug the leaks" so-to-speak. Models came into existence, such as the CD-57, with multiple, larger wheels, with from 25 to 47 pins per wheel. The number of lugs on the machine was increased from 27 to 40; and the concept of the "outer alphabet ring" was introduced. The purpose of these various modifications was naturally to improve the cryptographic security obtained from the system. But note the interesting fact that the newer CD-57 has no overlaps in the lugs! Here a new weakness is introduced into the system! And what of the "backers" of the HAGELIN CRYPTOGRAPH? What is their *faith* in the system? In Appendix I is a letter written by the manufacturer of the HAGELIN CRYPTOGRAPH. The letter, written, incidentally, in the early 1960's, is interesting. No doubt the writer of the letter is completely sincere, and no doubt a most intelligent invididual. But does he really prove the invincibility of the HAGELIN CRYPTOGRAPH?

But the author does want to be fair! The company manufacturing the HAGELIN CRYPTOGRAPH has never said, to the author's knowledge, that the HAGELIN CRYPTOGRAPH was or is invincible under all conditions. The inherent security provided by the HAGELIN CRYPTOGRAPH is no doubt understood by the manufacturer. And, indeed, as a tactical cryptographic system where the object of the system is merely to "delay" solution, the HAGELIN CRYPTOGRAPH is probably a good system. And there is another point to bring out. The year now is 1977. Modern cryptographic technology, the use of sub-miniature electronic components, "chips", etc. have made systems such as the HAGELIN CRYPTOGRAPH generally obsolete, so what we are really talking about is a system that though it is probably being used today is gradually disappearing.

APPENDIX I

Effect of computers on the security of Hagelin cryptographer type C-52

The two scientific marvels of our age are the missile and the computer, and there are several close parallels between them. Each represents a sudden advance which opens whole new fields for exploration and study; both are so new that we still cannot guess the magnitude and nature of their influence on our civilization. However, amazing as they are, both have predictable, technical outer limits. Today man flies around the earth in 90 minutes; he will probably fly to the moon in the next few years; but there are few of us who visualize manned flight to the outer reaches of the solar system, and almost none expect flight beyond the solar system. So it is also with computers. The highest operating speeds presently attainable are about 1/33 the speed of light, which is the maximum velocity of propagation in nature. In years to come, this speed will be improved, but almost no one believes that the theoretical maximum, the speed of light, will ever be attained in practice.

We are frequently asked by people who are unfamiliar with computers if cryptograms enciphered on our machine type C-52 cannot be deciphered with the assistance of these "giant brains". It is the purpose of this paper to demonstrate for those people that our machines have been designed so as to completely defeat the use of computers for this purpose at any stage of computer development in the forseeable future, and in fact even at the extreme outer technical limit of their potential development. It is of course assumed that our machine type C-52 is used in accordance with our advice as contained in our brochure 3153.

In order to decipher a cryptogram which has been enciphered on the machine type C-52 with a computer, we must undertake a process somewhat like this: Instruct the computer to assemble a combination of the variable elements of the machine type C-52, and beginning with some keywheel alignment attempt to decipher, say fifty letters of the cryptogram. This probably can be done on many computers. Having deciphered the message at our assumed combination of

the variable elements it is necessary to provide the computer with some form of test to determine whether the resulting text is really intelligible text, since clearly we will be unable to read the trial decipherments at the speed which the computer can produce them. How to achieve this on a computer is not clear at this time, but let us assume that it is achievable. If the first trial does not produce intelligible text, the computer will be instructed to try again at the next possible keywheel alignment, and so on until all the keywheel alignments have been tried. If the text has not been found at this point, the computer must try all possible wheel alignments all over again with the new inner settings. Sooner or later, the original clear text will appear. There is no theoretical obstacle to this process. There are only two sources of difficulty: One of these is that the total number of possible combinations of the variable elements in the machine type C-52 is so stupendous that in the number of false decipherments, many of which will be intelligible text, but not the true original message text. The feasibility of identifying the correct clear text is doubtful even if the necessary number of trial decipherments can be made. We are confronted with the classic problem that a large number of monkeys hitting keys on typewriters will ultimately type one of Shakespeare's plays. They will also type a fantastic number of other intelligible texts in their efforts and who is to say which was intended. Nevertheless, let us suppose that some way to overcome this difficulty can be found, and consider the second source of difficulty. The second source of difficulty is the time required to perform all of the necessary trial decipherments. In order to estimate the magnitude of this difficulty, we now consider how many trials must be made and how fast they can be performed.

It will be recalled that it is necessary to have the complete inner and outer settings of the machine type C-52, and the correct relative position of the typewheels, in order to decipher a message. The number of trials which our computer must make to ensure finding the correct decipherment of a cryptogram is equal to the total available combinations of inner and outer settings and relative positions of the typewheels. How many of these are there? The machine type C-52 comes equipped with a set of six keywheels, each carrying a pin disc. Each pin disc has a different number of pins. The number of pins on the wheels in the prime model is 29, 31,

37, 41, 43 and 47. The pins on each wheel may be set in either of two positions, called "active" and "inactive". Since each pin may be set in one of two ways and without regard to any other pin, the 29 wheel, that is, the keywheel carrying twenty-nine pins, may be set in any one of 2^{29} different ways, or over 500,000,000 combinations may be set on this wheel alone. Similarly, we can show that:

The 31 pin disc has 2^{31} combinations or over 2,000,000,000
The 37 pin disc has 2^{37} combinations or over 100,000,000,000
The 41 pin disc has 2^{41} combinations or over 2,000,000,000,000
The 43 pin disc has 2^{43} combinations or over 8,000,000,000,000
The 47 pin disc has 2^{47} combinations or over 120,000,000,000,000

Since the selection of the pin settings on one of these keywheels in no way restricts the selection on any other wheel, the total number of ways in which the pins may be set is actually the product of all of these numbers, or approximately 3.7×10^{68} which may be written:
370,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000.

This of course is based on every possible pin pattern being used. We recommend in our brochure 3153 that only patterns be used that have between 45-55% active pins on each wheel. This highly desirable limitation reduces the total number to 1.1×10^{67}, an insignificant change in a number of this size. It is believed that the computer would have to generate and reject these unacceptable patterns, it would not be feasible to completely avoid them. Nevertheless let us assume that it can be done.

The computation of the number of cryptographically different arrangements of bar lugs on the drum bars is somewhat complex. Suffice it is to say here that there are approximately 65,000 that are in accordance with our recommendations. Any one of these, of course, may be used in combination with any one of the enormous number of selections of pin settings which are possible, each combination being in effect a different machine, producing a different key from any other machine. Furthermore, the machine type C-52 is so constructed that the keywheels may be inserted into the machine in any order you choose. This increases the number of possible variations by a factor of 720. The rearrangement of the keywheels, even without changing any other element of the machine, will result in the generation of a completely different key than that which was produced by

the machine in the original arrangement. They are however not independent from the patterns of bar lugs on the drum bars, being indeed a much simpler method of effecting the same changes. Therefore the number of approximately 65,000 is the total for both variables.

Finally we come to the number of outer settings available, consisting of the keywheel alignments and the relative position of the two typewheels. In the prime model there are 29 x 31 x 37 x 41 x 43 x 47 = 2,756,205,443 possible keywheel alignments. There are twenty-six possible relative positions of the two typewheels, which may be selected without reference to the setting of any other element. In all then, the number of possible combinations of inner and outer settings is the product of the number of settings available for each variable element, or $1.1 \times 10^{67} \times 65{,}000 \times 2{,}756{,}205{,}443 \times 26 = 5 \times 10^{82}$. This is the number of trial decipherments of the cryptogram our computer must make in order to ensure that the correct decipherment is actually performed.

Let us turn now to the question of how fast we can perform this enormous task. In order to do this, it is necessary to touch briefly on the nature of large computers. (If additional information is desired, it is readily obtainable in literature from all manufacturers of large scale digital computers, as well as in the numerous books and articles published about computers and computer programming.) Every computer embodies a "memory", an "arithmetic" organ, a repertoire of "logical operations", and of course a means of getting data into and out of the machine. These components, however, are quite insufficient for the computer to be able to solve any problem. The so-called "giant brains" for all their speed and manipulative ability are incapable of independent thought. In order to get them to do the simplest job they must be "programmed" in minute detail by a man who knows exactly which steps should be taken under any possible conditions and in which order they should be performed. This program, which is introduced into the machine before the introduction of the data to be operated on, tells the computer where to put each item of data in its memory, what operations to perform in turn on each item, where in the memory to store the results of operations, and ultimately what items to print as an answer. A large percentage of a computer's operations consist of moving things around. Indeed, the actual arithmetic operations performed in a computer

are themselves achieved by either displacing 1's or 0's to the right or left, or by changing 1's to 0's or vice versa according to definite rules. Each computer is capable of a certain number of basic operations such as "add", "subtract", "multiply", "store in memory", "compare" (to determine which of two numbers is larger), etc. The important point to note is that the problem to be presented to the computer must be reducible to a great number of simple steps. The computer achieves its results not because of omniscience, but because of its ability to perform a myriad of simple tasks at prodigious speeds.

There are both theoretical and practical limits to this speed. One of the most frequent commands to be programmed is to shift data into or out of the memory. Let us assume a memory location is separated from the arithmetic organ by one meter, which would be a minimal distance. In that event the shortest time in which the entry within that location could possibly get to the arithmetic organ is 1/3000,000,000 of a second. This is because the maximum velocity of propagation in nature, the speed of light, is approximately 300,000,000 meters per second. In actuality, the time required to get an item out of one location and into another is far longer than this. A speed of 1/8,000,000 of a second is about the highest presently attainable. For our purposes we will suppose that our computer operates at the speed of light, since in no case can any greater speed be attained. If the machine type C-52 is proof against this, we may be sure it is safe from any computer which may ever be built.

The computer must now be programmed so that it can simulate the machine type C-52 and decipher the cryptogram at high speed for each combination of the variable elements. It must also be programmed to proceed systematically through every possible combination of variable elements. Each trial decipherment of our cryptogram if it is only fifty letters long will certainly require several hundred steps in our program. Each trial decipherment must then be tested to determine if it is acceptably intelligible text. This will additionally require a great number of steps in our program. The exact number of steps will depend on the design of the computer and the skill of the programmer. If we demonstrate that the time required to decipher our cryptogram is too great even if each trial decipherment and test for intelligibility could be performed in one step and each step at the speed of light moving one meter (so that 300,000,000

trial decipherments and tests for intelligibility could be made in a second), then it is clear that the time for decipherment and testing would be too great for any conceivable computer in existence.

If our computer can make 300,000,000 trial decipherments and tests per second, then it can make —

300,000,000 per second	x 60 =	18,000,000,000 per minute
18,000,000,000 per minute	x 60 =	1,080,000,000,000 per hour
1,080,000,000,000 per hour	x 24 =	25,920,000,000,000 per day
25,920,000,000,000 per day	x 365 =	946,080,000,000,000 per year

If we divide this last figure, the number of trial decipherments which can be made in a year, into the number of combinations of the inner and outer variables given above, we will have the absolute minimum number of years required to ensure the correct decipherment of our cryptogram. The answer so obtained is approximately 5×10^{67} years. If you hope at random to hit the correct answer by the time you go halfway, then the number is only 2.5×10^{67} years. This is after the fantastic concessions we have made to the speed and capabilities of these "giant brains". Either of these figures is clearly greatly in excess of the age of the earth. In fact, it is difficult even in this day and age to conceive of them. As is well known, time on computers is an extremely expensive item. Costs in excess of 1,000 Swiss francs an hour are not unusual. If you could buy computer time at a Swiss franc a year, the cost of exhaustively testing every combination of variable elements on our machine type C-52 would be beyond imagination.

Further, we are not trying to deprecate the great value of the computer to our modern civilization. We are not trying to deny that computers must be of great value to cryptanalysts. Their ability to handle great masses of data rapidly must make them a very valuable tool. But it must always be remembered that they do not think independently, and are tools indeed.

If one evaluates realistically the various ways by which an enemy can successfully recover a cryptographic usage, one is forced to the conclusion that by far the greatest source of danger is from unauthorized access to cryptographic instructions, key lists, and related documents. This can be achieved at any of a number of points; at the time of the

original drafting of the cryptographic documents, during their printing, during their forwarding, during their storage, or during their use. This may be with or without the collaboration of trusted personnel. In this day of ideologies the trustworthiness of personnel presents a serious problem. When one fully appreciates the limitations and costs of computer analysis, and considers what the expenditure of far less effort and cost could probably achieve in securing unauthorized access, one can appreciate the relative probabilities of the two attacks.

Far less dangerous than unauthorized access but next in magnitude of danger are poorly designed usages and errors committed by code clerks. The first can be avoided by a careful study of our brochure 3153. The second depends on the quality and experience of the code clerks.

When one considers all factors, it is clear that compared to the other threats to all cryptographic usages, the danger from computers can be considered insignificant.

BOOKS IN THE CRYPTOGRAPHIC SERIES

---

1 - **Manual for the Solution of Military Ciphers**, Parker Hitt
2 - **Cryptanalysis of the Simple Substitution Cipher with Word Divisions**, Wayne G. Barker
3 - **Elements of Cryptanalysis**, William F. Friedman
4 - **Statistical Methods in Cryptanalysis**, Solomon Kullback, Ph.D.
5 - **Cryptography and Cryptanalysis Articles, Volume 1**, edited by William F. Friedman
6 - **Cryptography and Cryptanalysis Articles, Volume 2**, edited by William F. Friedman
7 - **Elementary Military Cryptography**, William F. Friedman
8 - **Advanced Military Cryptography**, William F. Friedman
9 - **War Secrets in the Ether, Volume 1 [Parts I and II]**, Wilhelm F. Flicke
10 - **War Secrets in the Ether, Volume 2 [Part II]**, Wilhelm F. Flicke
11 - **Solving German Codes in World War I**, William F. Friedman
12 - **History of the Use of Codes**, William F. Friedman
13 - **The Zimmermann Telegram of January 16, 1917 and its Cryptographic Background**, William F. Friedman and Charles J. Mendelsohn, Ph.D.
14 - **Manual of Cryptography**, Luigi Sacco
15 - **Pattern-Word List, Volume 1**, Frederick D. Lynch
16 - **The Origin and Development of the Army Security Agency, 1917-1947**
17 - **Cryptanalysis of the Hagelin Cryptograph**, Wayne G. Barker
18 - **The Contribution of the Cryptographic Bureaus in the World War**, Yves Gylden
19 - **Course in Cryptography**, Marcel Givierge
20 - **History of Codes and Ciphers in the United States Prior to World War I**
21 - **History of Codes and Ciphers in the United States During World War I**
22 - **History of Codes and Ciphers in the United States During the Period Between the World Wars, Part I. 1919-1929**
23 - **The Riverbank Publications, Volume 1**, William F. Friedman
24 - **The Riverbank Publications, Volume 2**, William F. Friedman
24 - **The Riverbank Publications, Volume 3**, William F. Friedman
26 - **Cryptanalysis of an Enciphered Code Problem — Where an "Additive" Method of Encipherment has been Used**, Wayne G. Barker
27 - **The Voynich Manuscript — An Elegant Enigma**, M. E. D'Imperio
28 - **Manual of Cryptography**, British War Office
29 - **Principles of Modern Cryptanalysis, Volume 1**, Cipher Deavours
30 - **Military Cryptanalysis, Part I**, William F. Friedman
31 - **Speech and Facsimile Scrambling and Decoding, A Basic Text on Speech Scrambling**
32 - **Computer Simulation of Classical Substitution Cryptographic Systems**, Rudolph F. Lauer
33 - **Course in Cryptanalysis, Volume I**
34 - **Course in Cryptanalysis, Volume II**
35 - **The Origin and Development of The National Security Agency**

AEGEAN PARK PRESS, P.O. Box 2837, Laguna Hills, California 92653